DOCUMENT RESUME

ED 143 358 IR 005 132

AUTHOR	Westin, Alan F.
TITLE	Computers, Health Records, and Citizen Rights.
INSTITUTION	Columbia Univ., New York, N.Y. Dept. of Political Science.
SPONS AGENCY	National Bureau of Standards (DOC), Washington, D.C. Inst. for Computer Sciences and Technology.
REPORT NO	NBS Monograph 157
PUB DATE	Dec 76
CONTRACT	5-35886
NOTE	403p.; Some parts may be marginally legible due to small print of the original document
AVAILABLE FROM	Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (SD Cat. No. C13.44:157, $4.55. Add 25% additional for other than U.S. mailing)
EDRS PRICE	MF-$0.83 HC-$22.09 Plus Postage.
DESCRIPTORS	*Civil Liberties; *Computer Oriented Programs; *Confidentiality; Data Collection; Federal Legislation; *Health Activities; Health Facilities; Information Sources; Information Storage; Information Systems; Management Information Systems; Medical Record Librarians; *Recordkeeping; *Security

ABSTRACT

This is a report of an interdisciplinary team which: (1) examined the literature from medicine and health, law, computing, and social science; (2) conducted interviews with manufacturers, developers, health professionals, consumers, and public interest groups; (3) made site visits to health organizations using computers; (4) corresponded with health organizations; and (5) subjected the initial draft report to review by experts. Findings are in four parts: (1) description of medical data and citizen rights in three areas--primary health care, service payers, and health care reviewers, and social uses of health data; (2) patterns of computerization in health care in the three above areas; (3) profiles of six health-care organizations; and (4) the impact of computerization on health records, including a comparison of American progress in health care automation with experiences of six other democratic nations, and 12 management principles for health care data systems. An extensive bibliography and appendices of supporting documents are included. (Author/DAG)

****
* Documents acquired by ERIC include many informal unpublished *
* materials not available from other sources. ERIC makes every effort *
* to obtain the best copy available. Nevertheless, items of marginal *
* reproducibility are often encountered and this affects the quality *
* of the microfiche and hardcopy reproductions ERIC makes available *
* via the ERIC Document Reproduction Service (EDRS). EDRS is not *
* responsible for the quality of the original document. Reproductions *
* supplied by EDRS are the best that can be made from the original. *
****

ED143358

Computers, Health Records, and Citizen Rights

U S DEPARTMENT OF HEALTH,
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY

Alan F. Westin

Department of Political Science
Columbia University
New York, New York 10027

Sponsored by the
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

BEST COPY AVAILABLE

U.S. DEPARTMENT OF COMMERCE, Elliot L. Richardson, *Secretary*

Edward O. Vetter, *Under Secretary*

Dr. Betsy Ancker-Johnson, *Assistant Secretary for Science and Technology*

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Acting Director*

Issued December 1976

IR005132

Library of Congress Cataloging in Publication Data

Westin, Alan F.
Computers, health records, and citizen rights.
(NBS monograph ; 157)
Supt. of Docs. no.: C13.44:157.
Bibliography: p.
1. Medical records–Data processing. 2. Medical records–Access control. 3. Privacy, Right of–United States. I. Institute for Computer Sciences and Technology. II. Title. III. Series: United States. National Bureau of Standards Monograph ; 157.
QC100.U556 no. 157 [R864] 602'.1s [651.5] 76-608322

National Bureau of Standards Monograph 157

Nat. Bur. Stand. (U.S.), Monogr. 157, 401 pages (Dec. 1976)

CODEN: NBSMA6

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1976

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402 - Price $4.55

(Add 25 percent additional for other than U.S. mailing)

Stock No. 003-003-01681-1

FOREWORD

The use of computers to automate the information handling and record-keeping activities of Government and private organizations has brought the benefits of speed and efficiency to these operations. But it has also brought concerns for privacy stemming from the desire of individuals to control the collection of information about themselves and to exercise some measure of control over the use of that information.

Consideration of this basic issue -- how to utilize the benefits of technology while preserving individual rights -- has led to public policy regulating the use of personal information in credit reporting and Federal record-keeping.

Medical record-keeping is an area of special concern and broad impact for the development of sound public policy respecting privacy rights. Computer technology applied to medical records offers promising benefits of increased efficiency and improved health care. Advances in computer and communications technology could enable doctors in remote areas to have ready access to relevant information. The analytic power of the computer could be used in medical diagnosis. Medical research could be advanced through computer analysis of existing medical records.

However, this is a sensitive area where privacy concerns are strong. The National Bureau of Standards has sponsored this study of the privacy issues in medical record-keeping to advance understanding of the attendant privacy problems and their possible solution. This report, Computers, Health Records and Citizen Rights, is the result of a two-year research effort directed by Dr. Alan F. Westin, Professor of Public Law and Government, Columbia University. Dr. Westin is the co-author of Databanks in a Free Society, the landmark study of computers and privacy.

We offer Dr. Westin's recommendations to the health care and medical community for their consideration with the hope that these recommendations will help them develop policies that assure the protection of individual privacy rights. As the first thorough investigation of privacy issues in one sector of American society with sector-specific recommendations, it should provide helpful insights and a model methodology for studying privacy concerns in other areas. Towards this end, NBS and the Privacy Protection Study Commission are jointly sponsoring a follow-up study by Dr. Westin on personnel record-keeping practices.

Dr. Westin's study deserves wide review and careful consideration.

Ruth M. Davis

Ruth M. Davis, Ph.D.
Director
Institute for Computer
Sciences and Technology

PREFACE

This report has its origins in a Workshop on Privacy that met in Gaithersburg, Maryland, on February 8-9, 1973. Sponsored by the National Bureau of Standards and the Association for Computing Machinery, the group included experts from the computer community, law, the social sciences, public interest and civil liberties groups, federal executive agencies, and state legislatures.

Looking over the then-current state of the computers-and-privacy issue, the Workshop saw the United States entering a new phase of this problem. In the mid-1960s there had been early alarms about the potential impact of computer technology on citizen rights. This was followed between 1968 and 1972 by a period of empirical studies and legislative inquiries, probing just what the effect of computer use by organizations had been so far. Now, the Workshop concluded, having perceived the threats and mapped the issues, the nation was moving into a period of policy definition and regulatory action.

This new period would not be a short one. The Workshop was agreed that no legal or technological "fixes" could be applied quickly and comprehensively to automated personal data systems. The basic issues involved in organizational record keeping about people involved fundamental debates for American society over changing social values, new definitions of civil liberties, controversial government programs and business services, and shifting conceptions of proper and improper organizational authority. In addition, computer and communication technologies were highly dynamic; their continually changing capacities, problems, and opportunities would require very sensitive and flexible policy mechanisms, continually reviewed.

The Workshop saw the middle 1970's as a critical period in the development of sound public policies. The empirical reports and hearings of the 1969-1972 phase had alerted the media, the public, and national policy-makers to the need for action, and a wide variety of standards-setting proposals had been presented to legislatures, regulatory agencies, and organizational managers. Because many of these would involve far-reaching and expensive changes in the operations of major business and government functions in American society, they required a careful assessment; were they responsive to the real problems of citizen rights in a given situation? what was their potential impact on the informational needs of organizations and society? did they have the right blend of guiding principles, specific rules, realistic procedures, and enforceable remedies?

Most important of all, the Workshop was concerned that the public's clear desire for new privacy protections be channeled into law in time to catch the wave of large-scale systems building and adoption of fourth-generation computer-system technology that was expected to unfold in the middle and late 1970's. The participants at the Workshop were agreed that many of the proposed protections for individual rights would be "affordable" in dollar costs if these were spelled out as system requirements as the new systems were being designed, or as existing systems were undergoing major expansion. What would be painful or even unbearable, in terms of cost, would be to wait so long to formulate broadly-acceptable standards that information systems, as Dr. Ruth Davis put it, would have to be "retro-fitted" to conform to the new rules.

The Workshop speculated that new legislative policies in the middle Seventies would be likely to follow two main lines. One would be the enactment of broad "fair information practices" laws directed at the record-keeping of all agencies at a particular level of government, and covering both manual and automated data systems. (This approach, based on recommendations of the HEW Advisory Committee on Automated Personal Data Systems*, was soon well under way, and has already resulted in the enactment of the Federal Privacy Act of 1974 and similar laws in five states.) The second line of legislation would involve the passage of laws to deal with particular fields of record keeping, where detailed codes would be enacted to define citizen rights, work out balances among conflicting social values, and set specific mechanisms of supervision and enforcement.

To help both policy makers and systems developers evolve a set of basic standards during this early regulatory phase, the Workshop felt it would be valuable to conduct a series of interdisciplinary studies, following the approach of the National Academy of Sciences' Project on Computer Databanks.** That project had produced, for each field of organizational activity: (1) a description of the pre-computer baseline of record-keeping practices and citizen rights rules; (2) an empirical study of how computers were being used there and the effects this was having on the operations of personal record keeping; and (3) an analysis of policy alternatives available to insure that society's current expectations about citizen rights in that field were carried out, in both automated and manual data systems.

Looking over the main fields of organizational record-keeping about people, the Workshop identified a group of these that seemed to merit priority attention, based on factors such as the number of persons affected by these activities, the extensiveness of computer use, and the readiness of law and public opinion to take up regulatory alternatives. The fields selected were: banking and finance; credit bureaus and commercial reporting agencies; education; personnel practices; social and evaluative research; law enforcement and criminal justice; welfare; and health care.

The Workshop decided that the best course was to select one field and do it as a model study. Once this was conducted and published, its technique could be evaluated and, where it proved relevant, used by other researchers, organizational managers, and government study commissions. For reasons that will be noted in the Introduction, health care was selected to be the first field treated, and the Institute for Computer Sciences and Technology of the National Bureau of Standards was able to provide the funds to carry out the research.

This pilot project having been completed, the Institute is now sponsoring a second study, to be conducted during 1976-77. It deals with the personnel data systems of government agencies, business, and non-profit organizations, and is being funded jointly by the National Bureau of Standards and the federal Privacy Protection Study Commission.

---

*_Records, Computers, and the Rights of Citizens_, Report of the Secretary's Advisory Committee on Automated Personal Data Systems. U.S. Department of Health, Education, and Welfare, July, 1973, DHEW Publication No. (OS) 73-74.

**Alan F. Westin and Michael A. Baker, _Databanks in a Free Society_ (New York: Quadrangle, 1972.)

While many persons and organizations aided in the health care study (and are gratefully mentioned in the Acknowledgments section of the Appendix) two persons deserve to be noted here as the sustaining godparents of this work: Dr. Ruth M.Davis, Director of the Institute for Computer Sciences and Technology of the National Bureau of Standards, and Mr. Walter M. Carlson, first in his capacity as President of the Association for Computing Machinery, when the Workshop on Privacy was created, and since then as an advisor to N.B.S. Their patronage was in the best of the Renaissance tradition.

Alan F. Westin,
March 31, 1976

PROJECT STAFF

Director	Alan F. Westin, Columbia University
Consultants:	Michael A. Baker, Brooklyn College, City University of New York George J. Annas, Boston University Law School
Research Assistants:	Helene Toiv Richard Silberberg Jamie Broder
Writer/Editor:	Florence Isbell
Translations:	Daniel Lufkin
Administrative Assistants:	Lorene Cox Florence A. Erickson
Typist:	Barbara Delventhal

FINAL REPORT

Members of the project staff contributed background memoranda and site visit reports that were used by the Director to assemble the first draft of this Report, completed during the summer of 1975. This was reviewed at a conference of experts at the National Bureau of Standards in September of 1975. The report was then completely rewritten by the Director, with the editorial and writing assistance of Ms. Isbell.

The places in which the Final Report drew on staff memoranda have been noted at the appropriate point in this document. Since the final draft was done without staff consultation, responsibility for its organization, development, analysis, and recommendations is solely that of the Director.

A NOTE TO READERS

Though the Project on Medical Records and Citizen Rights is completed, the Director would welcome comments from readers about the facts presented, issues raised, and recommendations presented in this Report. Additional examples of intentional or unintentional violations of individual rights in medical records and health data would be particularly welcome, as well as new policy problems that may have arisen too recently to have been included in this study. Such material will be used in an updating of this Report to be published later, in a general forum available to all interested parties.

Please send such communications to:

Professor Alan F. Westin
Department of Political Science
729 International Affairs Building
Columbia University
New York, N.Y. 10027

CONTENTS

EXECUTIVE SUMMARY xi

INTRODUCTION 1

PART ONE: THE WORLD OF MEDICAL DATA AND CITIZEN RIGHTS 7

- Introduction 8
- Chapter 1. Zone I - Primary Health Care Records 12
- Chapter 2. Zone II - Service Payers and Health Care Reviewers 44
- Chapter 3. Zone III - Secondary Users of Medical Data. 60

PART TWO: ENTER THE COMPUTER 91

- Chapter 4. Trends in Computerization of Medical Data . 92

PART THREE: PROFILES OF COMPUTERIZING ORGANIZATIONS 123

- Introduction 124
- Chapter 5. Los Angeles County Medical Center 127
- Chapter 6. Martin Luther King Jr. Health Center 142
- Chapter 7. Kaiser Permanente Medical Care Program 164
- Chapter 8. The U.S. Indian Health Service 174
- Chapter 9. The Multi-State Information Service 187
- Chapter 10. Mutual of Omaha Insurance Company 201

PART FOUR: POLICY ALTERNATIVES 211

- Chapter 11. Assessing the Computer's Impact on Citizen Rights 212
- Chapter 12. Comparisons with Other Democratic Nations . 248
- Chapter 13. Policy Analysis and Recommendations 269

SELECTED BIBLIOGRAPHY 311

APPENDICES 341

1. Project Documents 342
2. Willis Ware Privacy Definitions 348
3. American Medical Association Model State Bill on Confidentiality of Health Care Information 350
4. IBM Medical Department Manual; Privacy Policy 357
5. HEW Draft Policies on Confidentiality for Professional Standards Review Organizations 367
6. American Civil Liberties Union Policy on Privacy of Medical Records 371
7. Summary of Ethical Health Data Centers Concept 372
8. Guidelines on Preserving Confidentiality of Medical Records, National Association of Blue Shield Plans 374
9. Policies and Recommendations for Policies, American Society of Internal Medicine 377
10. Members of the NBS/ACM Workshop on Privacy, February 8-9, 1973 379
11. Persons Attending Draft Report Review Conference, September 16-17, 1975, Gaithersburg, Maryland 380
12. General Acknowledgments 381

EXECUTIVE SUMMARY

Background

The concept of this model study originated in a Workshop on Privacy held in 1973 under the auspices of the Association for Computing Machinery and the Institute for Computer Sciences and Technology, National Bureau of Standards. The workshop believed it would be valuable to select one important area of record-keeping about people that was undergoing significant computerization and conduct a study that would identify the standards to be installed if society is to realize benefits from information technology without jeopardizing fundamental citizen rights.

Health care was chosen for the pilot study for several reasons. These include the universal impact of health-care records on the population; the fundamental reconsideration of goals and organization in American health care now taking place; the imminence of some kind of national health insurance plan; the increasing use of computers in health care; and current debates over the right of individuals to control the uses made of their personal health data. Funding for the study was provided by NBS.

Objectives and Methodology

The study had three objectives: to describe the pre-computer baseline of record-keeping practices and citizen-rights rules in health organizations; to conduct an empirical study of how computers were being used there, and the effects this was having on the operations of personal record-keeping; and to identify the principles and policy alternatives that would assure observance of citizen rights in emerging data systems, especially the automated ones.

Research was conducted by a small, interdisciplinary team under the direction of Alan F. Westin, Professor of Public Law and Government, Columbia University, beginning in the summer of 1974 and finishing in April, 1976. Examination of published literature from medicine and health, law, computing, and social science was augmented by interviews with major computer manufacturers, systems developers, and civil liberties, public-interest, consumer, and minority-rights groups. On-site visits were made to six representative health-care organizations using computers to handle personal records, with detailed profiles written of each organization. Correspondence and follow-up contacts were conducted with 70 organizations in the health care field. A draft report of the project's findings and recommendations was reviewed at a conference of experts in September of 1975, and then by approximately 50 outside reviewers. Following this, the Director and a professional writer re-wrote the report to reflect suggestions from the reviews and additional research. The final report's presentation and recommendations are solely the responsibility of the Director, and have not been subject to any clearance process by the project staff or the sponsor.

Part I: The Record-Keeping Baseline

As a baseline for studying the impact of computer use in health care, the report describes three different zones in which individual health data is used, each with different social norms and legal rules as to rights of privacy, confidentiality, and individual-access.

A. In Zone 1, primary health care, the report describes how medical records are used when a patient seeks help from a health professional, whether in a physician's office, a clinic or hospital, or in the health unit of an institution (colleges, corporations, the military, etc.). Though the importance of promoting full disclosure by patients to doctors has produced a long-standing ethical duty of confidentiality, and legal privilege against courtroom disclosure in most American states, the report shows how the growth of third-party payment for medical care, utilization reviews, and the growing uses of health data for social decisions have seriously weakened the observance of strict confidentiality.

The study found that the requirement of "informed consent" by patients to release of their primary care data is rarely well observed today. In part, this is because consent is often coerced by the threat of losing services or is assumed to be implied. Informed consent is also weakened because patients do not have a general right to see what is in their records, either before the data is released to third parties or as a matter of patient interest during regular care. Such problems of consent and access are being exacerbated in institutional health care, where physicians are employees of the institution and have mixed loyalties in handling patient information.

Overall, the main finding of this section is that identified patient information from medical records now flows regularly out of the primary care setting in ways that allow patients few controls over these disclosures.

B. Zone 2 covers use of medical data for payment of services and quality-of-care reviews. For the 190 million Americans whose bills are paid, in part, by private insurance coverage or government medical programs, the legitimate need for payers to determine eligibility, assess claims, and detect provider fraud has created a system in which reports of sensitive diagnoses and conditions are forwarded from primary care records. The study found considerable disagreement between medical professionals and the payers as to how much personal data from medical records really needs to be disclosed for the payment-review function, an issue of privacy that is particularly sensitive where review of psychiatric conditions is involved. The study also found that existing practices have not prevented leakage of personal medical data to persons whom the individual did not want (or consent) to have access to such facts, such as employers or fellow-employees in group health plans or government-agency employers. Questions have also been raised about how long personal data need to be retained by payers, and whether subscribers and aid recipients should have the right to examine their records.

As to utilization reviews and quality-care assurance, the study found that the use of these processes has not raised serious citizen rights issues up until now. However, the creation of the new PSRO review system for Medicare and Medicaid has generated considerable controversy over how patient and physician privacy will be handled.

C. In Zone 3, social uses of health data, the report details how American society has come to require the disclosure of personal health data to serve a wide range of other important interests, from employment, life insurance, welfare, and rehabilitation to law enforcement, social research, licensing, and prevention of child abuse. How to adjust the balance between claims of medical confidentiality and legitimate social programs clearly requires careful assessment area by area. However, the report finds rising criticism of the use of health data in many of these areas to make what are challenged as stigmatizing and discriminatory judgments about people. This involves disabilities against persons who have had psychiatric treatment, or various kinds of non-disabling physical ailments, or whose practice of homosexuality is supposed to make them greater health risks than heterosexuals, or women who have had abortions, or persons who want to keep confidential the fact that they are undergoing drug or alcohol rehabilitation. In the post-Watergate mood, the protests have been particularly sharp when it is government agencies that insist upon recording such sensitive health data and using it to control the individual's rights and opportunities.

D. In all three zones, the report concludes that traditional laws and organizational policies have not kept pace with the new flows and uses of health information throughout our society, and that standards to resolve the growing policy debates are lacking in many sectors of the national health care system. This leaves computer systems developers in health care without clear policies to guide the automation of files and assemblage of data systems.

Part II: Patterns of Computerization in Health Care, and Their General Citizen Rights Implications

A. The study examined current patterns of computer use in each of the three zones. While automation in Zone 1, primary care, has been slight in the physician's office, the crush of paperwork in large clinics and hospitals for billing and accounting, third-party payment, reporting duties, lab tests, and similar areas has produced extensive computer applications. The development of integrated-file, databank-oriented hospital information systems, though much discussed in the technical literature and the general press, remains largely at the pilot stage where it is being attempted. Overall, the main effects on citizen rights of computer applications to patient records in primary care has been to increase the systematic collection, recording, and centralization of patient data, both social and medical; this tends to sharpen questions of just what data ought to be recorded, how long it should be kept, what release procedures are to be used, and whether patients will be able to inspect what is in their records.

B. In Zone 2, service payment, computer use has been widespread throughout the health insurance industry, with increasing amounts of patient data being collected and stored in their files. While no special problems of leakage have appeared as a result of computer use per se, unclear policy definition as to what identified data should be collected for payment reviews and who else should get such data are central issues here.

C. In Zone 3, the report did not try to describe how computers are being used in the dozen or so major areas of social activity that use health data to support their functions. However, one Zone 3 area whose computer use was examined was automation by government health-administration agencies, which have increasingly been creating controversial databanks of identified patient data for planning, evaluation, and research purposes.

D. Overall, the survey of computerization in health care found that automation has not been as extensive as in fields such as banking, law enforcement, or taxation, though it is growing steadily in use and sophistication. Some observers feel that a sharp take-off in health computing is about to occur, as a result of rising costs requiring closer record-keeping controls and the likely prospect of national health insurance. However, expansion of computer use for hospital information systems is not seen as imminent, owing to the absence of conceptual models of how information uses in the hospital could be reorganized in ways that would be both cost-effective and acceptable to health professionals and the public.

Part III: Profiles of Computerizing Organizations

To examine how organizational policies and computerization efforts are affecting citizen rights, the study presents detailed profiles of six organizations involved in automating personal health records.

A. Los Angeles County Medical Center is a large county facility primarily serving the urban poor and minority groups of East Los Angeles. It is an average or "mainstream" computer user, with a project to automate medical records in a databank to improve patient care. The profile shows that the factors which shape basic citizen rights policy are the pressure on the Center to recover costs, leading to an emphasis on collecting extensive personal data; the Center's cooperative relations with local government and police officials seeking patient data; and a "ghetto-crisis" medicine that has no place for such "luxuries" as giving patients access to records or obtaining truly informed consent before releasing patient information. Computer use at the Center incorporates these basic problems and reactive policies. The report concludes that it would take a combination of new patient-rights legislation and reorientation of staff resources and priorities to install significantly greater citizen rights in the Center's operations, and that this will not take place any sooner — or later — as a result of the Center's plans for further computerization.

B. The Dr. Martin Luther King Jr. Health Center is a federally-funded, private facility providing ambulatory care in a high-poverty area of the South Bronx, in New York City; it supplies comprehensive, family-centered health care to approximately 40,000 registered patients, with a staff of 450. Computer use has been of the "mainstream" variety, but this Center's emphasis on the health-team approach to care, its heavy use of community people in staff and decision-making, and its innovative policies and practices as to patient rights presents a fusion of computer technology and citizen rights that is very different from that of Los Angeles Medical Center, even allowing for the differences between acute and ambulatory care. The report regards as exemplary the King Center's philosophy that machines must facilitate rather than weaken the Center's basic commitment to patient dignity and social advocacy.

C. The Kaiser-Permanente Medical Care Program offers the experience of a five-year, "leading-edge" project on computerized patient records in the Oakland-San Francisco area, which was aimed at eventually creating a "hospital information system." As a pre-paid medical plan that is both medical provider and insurer, Kaiser serves primarily middle class and unionized workers, and its health care has been excellent. It gave careful and effective attention to citizen rights in the Oakland project, especially as to access controls over patient data stored in the computer system. The federal grant to Kaiser was not renewed in 1973, and while the report discusses the different explanations for this withdrawal of funds, the treatment of the Kaiser project underscores the uncertainty of funding and organizational problems that face leading-edge projects in the hospital field today.

D. The U.S. Indian Health Service operates an advanced health information systems project in Tucson, Arizona that maintains integrated, on-line medical records for approximately 10-12 thousand Papago Indians in Southern Arizona. Though this has helped greatly with some of the special problems of record-keeping raised by an itinerant patient population, and has generated excellent administrative reports, the computer project has not been able to do much about the desperate medical condition of American Indians in Arizona and elsewhere and the glaring inadequacy of federal funds and facilities being provided to cope with these health problems; in fact, the improved reporting only highlights the problems more sharply. The study found that the Indian Health Service has been sensitive to special Indian attitudes on privacy but that problems of confidentiality of records and issues of patient access remain. These are now being addressed under the new provisions of the Federal Privacy Act of 1974, and the report notes some of the initial problems that have arisen in implementing those policies in the Indian Health Service.

E. The Multi-State Information System (MSIS) is an automated information system containing records on about 400,000 mental patients. It serves both administrative and research purposes for participating institutions (primarily state and private mental health facilities in the Northeast) and the research activities of the developer and manager of the system, the Information Sciences Division of Rockland Research Institute, a state facility in Orangeburg, New York. MSIS has pioneered in securing a special state statute to safeguard the confidentiality of the sensitive psychiatric data that it stores. But it has also been the target of considerable attack because it creates a new type of centralized, regional databank of identified psychiatric information, separate from and in addition to the records kept in the participating mental facilities. The report notes that prividing strong safeguards for such regional and national information systems containing special medical data is especially important in the post-Watergate climate of public concern over government abuse of confidential records.

F. Mutual of Omaha is a profit-making, multi-line insurer which is not only the largest provider of private health insurance in the United States but also an advanced computer user. The report traces the citizen rights issues involved in underwriting decisions and claims investigation at Mutual, and the compliance of the firm with important protective legislation such as the Fair Credit Reporting Act and the Federal Privacy Act (the latter because Mutual is a fiscal intermediary under several federal health-payment programs). The report finds that Mutual's use of computers has followed rather than altered its basic confidentiality policies, has probably enhanced the security of subscriber data, and has not interfered with Mutual's compliance with federal laws. The key issues of citizen rights facing Mutual and all other health insurers, the study notes, are issues of social policy, such as how far American society will insist upon socializing certain risks (insurance of homosexuals, forbidding "objective" but racially-based standards, etc.) and thereby alter the collection and use of personal data that now support industry practices in these areas.

Overall, the six profiles showed that the deployment of computing and communication by health organizations is still essentially a matter of organizational artistry, not management science. Computerizing requires managers to exercise choice in selecting the files and data flows to automate, arranging configurations of hardware and terminals, writing software, defining operator-machine relationships, setting patterns of data-sharing inside and outside the organization, deciding on levels of organizational monitoring and reporting, and reviewing what types of data collection, patient consent, and access-to-record rules the organization traditionally provided and what it will now provide in its automated system. While some important effects are being exerted by new laws, the real locus of decision-making today as to how citizen rights will be treated in these new systems still lies with organizational managements.

Part IV: Policy Alternatives

Computer Impact on Citizen Rights

For crucial backdrop, the report notes the social setting in which health-care computerization is unfolding: distrust of the computer by various disadvantaged groups as an instrument that continues discriminatory practices against them; widespread public skepticism about the delivery and/or value of many "data-based" government social programs; general distrust of the government's motives and respect for confidentiality rules, in the post-Watergate mood; rising "consumerist" challenges to many traditional practices in the health field; and a clear public consensus by the mid-1970's that rules to protect citizen rights must be instituted when large-scale systems of personal data are instituted by government agencies and private organizations.

Turning to the impact of computer use in health care, the report found that most cases of actual harm involving individuals were still arising from manual records. These remain the places where most sensitive medical records and health data are stored and through which transfers of data are still effectuated. The project also found that, as a whole, computerized health records are more securely kept and processed today than manual records, with instances of leakage or misuse discovered by the project almost always taking place in manual files.

The report concludes that the main problem today with use of automated medical records involves potential harm - the creation of health data systems that many health professionals, citizen groups, and individuals directly affected by such systems consider to be threats to basic rights.

The report then presents descriptions of some two dozen selected episodes in which government agencies or private organizations either announced or set up health data systems only to encounter concerted opposition from various local groups for failing to define and safeguard citizen rights in those ventures. Among the data systems described are state health department discharge reports; state mental health department case reporting files; state welfare department client-services reports; medical notations in juvenile court and police records; state data systems on handicapped children; state "abortion surveillance" reporting; city and state registries for fetal death, child abuse, drug prescriptions, and narcotics treatment; state databanks consolidating records on all social services received by state residents; state beneficiary-explanation mailings to identify provider fraud; and the Medical Information Bureau system for life-insurance company data exchange.

After analyzing what had happened and why in these episodes, the chapter concluded:

"Most computerized health data systems are being created or expanded without sufficient consultation in advance with groups representing citizen rights and doctor-patient interests, and without some kind of proceeding open to the general public. Most data systems lack sufficiently developed analyses of how much and what kind of identified personal data they really need to perform their function. Even when properly defined, most data systems fail to adopt sufficiently precise standards of confidentiality, controlling uses within the organization and release of identified data to third parties. When it comes to rules for permitting patient access to their own records, very few computerized organizations have adopted procedures responsive to those patients who ask for and insist upon access....What we have today are ambiguous and ill-defined systems that leave people uncertain and fearful about their capacity to control the circulation of their medical and health data."

Comparisons With Other Democratic Nations

To compare American progress in health-care automation and protection of citizen rights with the experiences of other industrial democracies, the report surveyed these issues in approximately two dozen other nations, presenting country reports on six of these: Britain, Canada, West Germany, Australia, France, and Sweden.

As far as computer use, the main conclusions of the survey are that automation is extensive and well-established in the health institutions of these nations but is still heavily centered on administrative and laboratory applications in hospitals, and administrative applications in health-insurance programs; that leading-edge hospital systems and regional health information systems are still in experimental stages with their work on patient records, though these are aided by the presence of unique citizen numbering practices; and that automation efforts have encountered many of the same problems of proving cost-justification, overcoming professional opposition to computers, and competing for funds with other social programs as in the United States.

As to protection of citizen rights, the report finds that public debates over protection of privacy have followed the same patterns in these nations as in the United States; that many of these nations have developed principles to be followed in computerized data systems that closely resemble the American concepts of fair information practices established by the Federal Privacy Act of 1974; and that it is in the mechanisms to install, administer, and enforce those principles that the main differences lie between the United States approach and that of other industrialized democracies. As a prime example, the report describes the data inspection and registration approach taken by Sweden and how this has been applied so far to medical records and hospital systems. This section concludes by noting that most Western nations are at the same stage as the United States in this area, aware of the problems but just beginning to enact and administer protective laws to safeguard individual rights in steadily-expanding health data system.

Policy Analysis and Recommendations

The concluding chapter begins by stating that no single law, judicial ruling, regulatory action, or organizational policy can hope to deal with the tremendously varied and complex issues of citizen rights in health record-keeping; it will take a mosaic of policy actions, over time, to do what is needed. However, the report stresses that these actions must begin to be taken now, rather than assume there is time to wait until national health insurance is enacted or a reorganization of the American health-care system is completed.

As background, the report presents a set of concepts that have developed during the past few years as basic principles to be followed by any large-scale data system using personal records. These are: adopting a "contract" as well as civil-liberties theory of informational privacy; recognizing certain special dangers in automated data systems; setting primary responsibility with the "keeper" of each data system; identifying a legal duty to take reasonable care in the use of personal data and specifying the standards required to meet such a duty in each field; issuing public notices and privacy-impact statements when data systems are created and expanded; and providing independent, outside reviews of the operations of each data system.

Applying these concepts to health data systems, the report presents 12 major principles that ought to be followed in the management of data systems in the health field, and discusses alternative ways that these principles might be carried out. The 12 principles are:

1. There should be a procedure for issuing a public notice and privacy-impact statement whenever an automated data system is created in the health field, filed with an appropriate outside authority and communicated to any continuing population of individuals whose records will be affected.

2. Socially-acceptable standards of relevance and propriety in the collection of personal data should be worked out for data systems in each of the three zones of health-data use, through public discussion and appropriate policy-setting mechanisms.

3. Individuals should be given a clearly-written account of how their personal information will be used whenever they are asked to supply personal information to a health data system, along with the procedures to be followed before any uses are made of their data other than those originally specified.

4. Forms used to release personal information from a health data system should be for a specific purpose, describe the information to be released, and should be limited in time, and the individual's consent to such releases should be informed as well as voluntary.

5. As a general matter, patients should have a right to full information about their health conditions. Where health data is to be used to make judgments about service payment and claims, or in any non-medical social and governmental programs,

the individual should have an absolute right to inspect what is to be released from his/her record. In chronic and acute care, patients should also have a right to see any part of the medical record, including the medical professional's working notes, if the patient insists upon this after the medical professional has had a chance to explain directly to the patient why he or she feels that such disclosure would not be in the patient's best medical interest. A special procedure is suggested for patient-access problems in psychiatric care.

6. Managers of health data systems must take steps to see that personal records are as accurate, timely, and complete as the uses to which they are being put require for protection of individual rights.

7. Data security measures must be taken to control access according to the policies set by law or by management, and the adequacy of those measures will be measured by the previous history of threats to data confidentiality in that type of organization.

8. Health data systems should conduct special orientation and training programs to inculcate respect for citizen rights among their staffs and to deal with problems that may arise.

9. Each health data system should prepare and distribute a patient's rights handbook, and install a readily-available and independent patient rights representative in the organization.

10. Because new issues are posed whenever health data systems adopt new file applications, there should be provision for periodic independent review of each system.

11. Special efforts should be made so that confidentiality rules do not interfere with the public's right to know what is being done by government agencies or by private recipients of government funds, and to carry out critical oversight functions in the public interest.

12. The importance of health-care evaluation and medical research calls for developing special procedures so that these activities can be carried on without jeopardizing citizen rights.

Recognizing that the job of refining and applying these principles is a long-range task, the report notes some areas of priority for current action. On the legislative front, these include activities such as removing the exclusion of medical information from consumer rights under the Federal Fair Credit Reporting Act; adopting new state medical confidentiality laws and medical-research privilege statutes; supporting enactment of fair information practices laws in the 45 states that do not have these; and writing more explicit citizen rights guarantees than have yet been included in the major pending bills to create national health insurance. On the judicial front, the report recommends development of a legal duty by health organizations to manage their data systems according to standards of reasonable care, evolved by judicial definition in test cases. For organizations operating health data systems, the report urges a full-scale "privacy audit." It also urges sustained activity by public interest groups, noting particularly the critical role played during the past few years by the American Civil Liberties Union, and the important potentiality in the newly-formed National Commission on Confidentiality of and Access to Health Care Records.

The report concludes with this comment:

"It is the custom of Americans to believe that no 'lady-or-the-tiger' choice has to be made between science and liberty. For 200 years, in the tradition of Franklin and Jefferson, we have hammered out legal rules that allowed each successive wave of invention to realize its potential, but also required each to be brought under the rule of law. Sometimes it took a while for the principles of regulation to become clear, and we have come to realize that the awesome effects of contemporary technology give us less lead time for social learning and regulatory response than we had in earlier eras. But that is the challenge we face, and there are promising signs that our society understands how important it is to develop, soon, the standards by which we can pursue the benefits of both science and liberty in the field of health care."

xx

ABSTRACT

This report investigates the impact of computers on citizen rights in the health record-keeping area. Under Dr. Alan F. Westin's direction, from July of 1974 to April of 1976, a small interdisciplinary team did the following: (1) examined published literature from medicine and health, law, computing, and social science; (2) conducted interviews with major computer manufacturers, systems developers, health professionals and civil liberties, public interest, consumer, and minority-rights groups; (3) made on-site visits to six representative health-care organizations using computers to handle personal records; (4) corresponded with 70 organizations in the health field; and (5) subjected an initial draft report to review by a conference of experts in September 1975 and subsequently by about 50 outside reviewers. The findings of this investigation were then combined into this four-part report. Part One describes the world of medical data and citizen rights within the framework of three zones--primary health care (by health professionals), service payers and health care reviewers, and social uses of health data (such as in employment, life insurance, and welfare); Part Two treats patterns of computerization in health care in each of the above zones; Part Three contains the profiles of the six health-care organizations that were studied in depth; and Part Four analyzes the impact of computerization on personal health records, presents comparisons with six other democratic nations, and states 12 recommended management principles for health care data systems. The report also contains a 28 page bibliography and twelve appendices with support documents and information.

Key Words: Citizen rights; computers; confidentiality; data systems; health records; information policy; management principles; medical records; privacy; record-keeping practices; security.

INTRODUCTION

Background and Objectives

In considering which major field of record keeping about individuals to use as the subject for our pilot study, we had little trouble in selecting health-care as an ideal candidate. Since every person undergoes medical treatment from infancy to death, health-care is a universal experience. Since the use of health-care data affects everyone's rights, benefits, and opportunities in the larger society, this presents all the subtle and difficult problems of how to regulate secondary uses of personal information. Though there had been some valuable writing about medical data and privacy by 1974, when this project began, the field had not been as extensively studied and publicly discussed as many others, such as law enforcement or credit reporting. Finally, there was reason to believe that the potential existed for developing consensus among medical professionals, policy-makers, and public interest groups as to the emerging civil liberties problems in health-data systems and the range of alternative policies that could deal effectively with those dangers.

Thus we chose health care. We did so with an awareness that the field was in a state of major change in three basic dimensions: the goals and organization of the nation's health delivery system; the application of computer technology in medical services and health-data reviews; and the status of the individual's right to control the uses made of his or her personal health data.

1. That our health care system is moving toward a fundamental reorganization needs little documentation. The soaring costs of health care, the uneven and distorted distribution of services, and rising public expectations as to health care have carried us to the brink of enacting national health insurance. Such a new method of financing American health care for most citizens will increase the federal role in paying for and in assuring the quality of medical care; will foster new insurance and organizational mechanisms providing supplements to the federal minimum system; and will lead to basic reconsideration of the ways in which health care is conceived, organized, delivered, evaluated, and publicly regarded. Wholly apart from national health insurance, leading voices in the health field have called for reshaping health institutions, linking environmental controls more closely to preventive health, experimenting with new forms of health screening, and launching far more comprehensive research into health matters than has been traditional in our society. More changes are expected during the next decade in our health care system than we have seen since World War II, or even longer.

2. Computer applications in health care are expected to undergo a similarly major shift. The new financing and payments mechanisms under national health insurance will explode claims processing, and the requirements of quality-care review already under Professional Standards Review Organization (PSRO) for Medicare will add tremendously to the transactional flows. These two developments alone account for the judgment of most computer forecasters that the area of health-care computing is about to undergo the kind of expansion that marked data processing in banking or law enforcement in the past decade.

Many experts believe that the next decade will see major advances in a host of application areas in health care that have been slow in unfolding so far —

hospital information systems, regional health data systems, special health registers for problem areas, lifetime personal medical histories, and many others. The citizen in 1980 or 1985, it is predicted, will feel the presence of computers continually throughout his or her health-care contacts, from the terminal that will take a medical history in the doctor's office or clinic to the on-line medical history that will be available whenever or wherever health catastrophes occur to a person, or to the machines that will, Star-Trek style, monitor vital signs and changes as patients lie in hospital beds.

3. Finally, as we noted in the Preface, the United States is now entering a period of new legal regulations and organizational policies as to personal privacy. The Federal Privacy Act of 1974 was a fundamental breakthrough, representing Congress' finding that new legal standards should be installed to protect citizens from misuse of personal data by federal agencies. A Privacy Protection Study Commission created by the 1974 Act has been charged by Congress with the duty of conducting a broad two-year study of privacy and record-keeping in state and local government and among private organizations, with a long list of particularly sensitive areas to be explored, one of which is the medical field.

Where medical records are involved, serious questions have been raised before the public, in the post-Watergate setting, as to how confidentiality can be assured in a national health insurance system, as well as what is happening already to the confidentiality of personal medical data as computerized data collection and exchange has spread in the health care environment. Another aspect of citizen rights in health care — the right of patients to see the medical records assembled on them — is becoming a well-articulated demand of various consumer-oriented and civil liberties groups, paralleling the "right-of-access" issue in many other information systems.

Predictably, there are divergent views among observers as to the nature and extensiveness of threats to privacy in various new health care programs, and in the growth of automated data systems. But there is widespread agreement that dealing wisely and effectively with the privacy "issue" is a vital matter, not only to the public's confidence in new health care institutions in the coming decade but also to the protection of fundamental citizen rights.

The time is ripe, therefore, for focusing expert and public attention on these issues before changes in health care financing and review are enacted, before the new wave of computer applications and information systems unfold, and before arrangements to incorporate national patient identifiers and file-linking arrangements in the health field are put into place. Helping to sharpen that focus, through an inter-disciplinary research effort and preparation of an agenda of policy alternatives for the next decade, is the objective of this report.

Basic Assumptions

We began our analysis of computer impact in the health-care area with some guiding assumptions derived from the National Academy of Sciences' study of computers and privacy in 1969-1972. (That study had included health-care organizations among its 15-20 major areas of personal record-keeping in American society, with site visits that covered hospitals, health insurance companies, local and state government health agencies, employee medical departments maintained by private employers and government agencies, and medical services in schools and universities). We regarded the findings of the NAS report as general probabilities, subject to verification or alteration on the basis of our detailed researches into health-care automation in 1974-75. The NAS findings we considered particularly relevant to our project were these:

A. That computerization of personal data in the great majority of organizations carries forward whatever legal rules, social norms, and organizational policies as to citizen rights (for better or for worse) that prevailed in each type of organizational activity in its manual-record milieu. That is, computerization as such has not led to either "stronger" or "weaker" policies with regard to citizen rights. Unless such forces as new laws, public protests, or pressures from within by professional workers, intervened to influence organizational managements, automated systems adopted existing policies as to what information was collected, how it was used within the organization, with what outsiders the data was shared, and what provisions were made for access and review by the individual.

B. However, computerization spread through the world of organizational record-keeping during a period of drastic change in American values and social allocations. In the past decade, groups formerly discriminated against in the awarding of society's benefits and opportunities have demanded and won recognition of their right to equal treatment. Essentially, this means that the collection of personal data by government agencies or private organizations on matters of religion, race, sex, political activity, cultural style, or sexual preference is no longer considered legitimate unless it can be shown that such data are not being used by such organizations to make discriminatory judgments. Moreover, the record systems of most large organizations still contain a great deal of subjective and judgmental data about individuals collected in the "earlier era"; unless systematic purging of such data is undertaken in both manual and automated files, there are serious risks that individuals will continue to have judgments made about them on the basis of improper information. Furthermore, the public had registered in the 1960's its clear dissatisfaction with the creation of secret data systems about citizens, whether by police or commercial reporting agencies, as well as the making of evaluative decisions about individuals in reliance on records that the individual did not have an opportunity to inspect, with procedures for correction should there be inaccurate, incomplete, or misleading information in them.

C. The NAS study found that computer use had not resulted by 1972 in the merger of all files within an organization or at a level of government in the kind of "one-big-databank" approach that was advocated by some computer enthusiasts in the late 1960's and early 70's, and which had been properly viewed with alarm by social commentators aware of how little law was then available to control such greatly enhanced data systems, if they did come into existence.

D. The NAS study found that automation seemed to be creating certain effects that did deserve close attention. In most organizations, computerization was leading to faster transmission of data and faster decision-making; more complete and up-to-date records on persons; greater "massage" of personal data once it was collected; the creation of some large centrally-directed regional or national data networks; and the creation of some large personal data systems that would probably have been too costly or cumbersome to have been initiated under manual procedures.

None of these effects were seen by the NAS study to be automatically bad for civil liberties, but they did enhance the efficiency of governmental and private organizations in the use of personal data at a time of high public distrust of government and private institutions, especially for their intrusion into zones of personal and group privacy. This made even more imperative the establishment of clear public policies to control the automated data systems that would be steadily expanding, and growing far more sophisticated, in the late 1970's and 80's.

E. The NAS study concluded that in the mid-1970's, most controversial issues of citizen rights in record-systems would still involve manual records rather than the automated systems. This was essentially because the more narrative and subjective records in each type of organization, which usually involved the most critical civil liberties issues, had not yet been automated. Thus when citizen rights questions were addressed, the NAS study concluded that the first priority was to re-examine data policies without regard to whether the storage and processing medium was manual or automated. Once proper rules had been set, policy-makers should then address what special safeguards and procedures were necessary for automated files, and set these into place as general system requirements.

Methodology

We followed the general methodology used by the National Academy of Sciences' Project on Computer Databanks.* As applied to the health care field, this entailed four steps:

1. Documenting the patterns of record-keeping about people that prevailed in the health care field before automation arrived, including the realities of organizational behavior and the civil liberties rules that were applied in that milieu.

2. Describing the reasons why health care organizations have moved to adopt computer technology, tracing the changing patterns of computer applications down to the present, and presenting concrete case studies of organizations that have undergone these developments, including their handling of citizen rights issues.

3. Identifying the effects of computerization on the status of citizen rights in the health area, including in this estimate an analysis of changing social norms, public expectations, and legal conceptions of these rights during the highly dynamic period of the past decade.

4. Posing the policy alternatives that face American society in this field if new standards and procedures are to be adopted, by organizational initiative and/or public regulation, to assure the vitality of citizen rights guarantees in the increasingly computerized ethos of health care record keeping.

We have also employed the basic research techniques of the National Academy of Sciences' study. Following a thorough inspection of the published writings on our topics in the literature of health-care, law, computers, and social sciences, we held briefing sessions with three major computer manufacturers (UNIVAC, I.B.M., and Honeywell) to discuss computer applications in health care. We then made site visits to six organizations whose experiences would provide insight into the way computerization and citizen rights developments were taking place in the real world; these site visits were written up as case studies and appear in Part III of this Report.

---

* Alan F. Westin and Michael A. Baker, Databanks in a Free Society (N. Y.: Quadrangle, 1972).

For general background, we contacted about 70 organizations in the health care field, soliciting any policy statements, research studies, or other material that they had on the issues of confidentiality and computerization. We also conducted a survey of the national and state affiliate offices of the American Civil Liberties Union, to obtain instances of complaints about violations of confidentiality or refusals of patient access to records. Similar inquiries were made of public-interest law firms, consumer organizations, minority rights groups, and regulatory agencies. Another technique that we used was to devise a form soliciting reports of violations of citizen rights in the use of personal medical data, in either manual or computerized settings; we distributed this form at several national meetings of health care organizations during 1974-75.*

For comparisons with trends in computer use and citizen rights protections in the health care systems of other democratic nations, we corresponded with medical societies, government experts, lawyers groups, and civil liberties organizations in about a dozen nations. We also had contacts with the Computer Utilization Group of the O.E.C.D. in Paris, through its director, Dr. Hans Gassmann. The patterns of experience in a group of selected nations appears in Chapter 12 of the Report.

We regarded a careful review of the first draft of this report by a group of experts representing the interested parties in health care and citizen rights to be a vital part of the project methodology. This was not only for the usual purpose of obtaining corrections of fact and reactions to specific judgments and recommendations but also to test the range of agreement as to problems and solutions among medical specialists, government health officials, lawyers, civil liberties groups, computer experts, and similarly important participants in the standards-setting process.

This was done in two parts. On September 16-17, 1975, a review conference of 35 participants, under the chairmanship of Dr. Vernon Wilson, was held at the National Bureau of Standards, in Gaithersburg, Maryland. Copies of the report were also sent out for written comments to a group of about 50 additional specialists. (A list of these reviewers is contained as an Appendix, and we are very grateful to them for having made such a useful contribution to the project.) We found that there was, indeed, a very large area of agreement among these reviewers on how to approach the issues in the field, and we discuss this situation in the final chapter.

Following the reviews, the report was completely revised by the Director and Ms. Florence Isbell, during the period from September, 1975 to March, 1976.

Definitions

A last few introductory words are in order to define three terms used in this report to represent the main civil liberties interests of the citizen in personal records.

---

*See Appendix I for lists of organizations contacted, sample forms, etc.

1. *Privacy* is the question of what personal information should be collected or stored at all for a given social function. It involves issues as to the legitimacy and legality of organizational demands for disclosure from individuals and groups, and the setting of balances between the individual's control over the disclosure of personal information and the needs of society for the data on which to base decisions about individual situations and to formulate public policies.

2. *Confidentiality* is the question of how personal data collected for approved social purposes shall be held and used by the organization that originally collected it, what other secondary or further uses may be made of it, and when consent by the individual will be required for such uses. It is to further the patient's willing disclosure of confidential information to doctors that the law of *privileged communications* developed. In this perspective, *security* of data involves an organization's ability to keep its promises of confidentiality.

3. *Individual access* is the issue of when individuals should know that a record has been created about them, and when they can examine it in order to check its accuracy, completeness, and the uses being made of it. Fundamentally, the claim to access rests on the due process of law guarantees of the American legal system.*

There are other citizen rights issues in the field of health care that we do *not* cover here, basically because they are not record-keeping problems and are not being affected significantly by changes in information-handling technology. These include the individual's right to treatment, informed consent for medical experimentation, the right to elect death, and similar important questions.

Finally, we will use both the terms *medical records* and *health data* in our discussions. By medical records, we mean the formal record of a patient's reception, treatment, and progress in primary care settings, usually taken by various health professionals; this will include any personal, family, or social histories acquired for patient-care purposes. We use health data to describe any information about a person's physical or mental health, whether originating in a medical record or other source, that is used to make a judgment about an individual's rights, benefits, and opportunities in situations other than direct health care.

Acknowledgments

As with all works of large-scale research, this study would not have been possible without the generous cooperation of many people. Their names have been included in Appendix 12, with our genuine appreciation.

---

* For further refinements of these concepts, we include in Appendix 2 a very useful set of "Privacy Definitions" compiled by Dr. Willis Ware.

Part One

The World of Medical Data and Citizen Rights

INTRODUCTION

To measure the impact of new computer and communication technologies on health records and citizen rights, we need a set of baselines. In this case, we need three baselines:

1. How were medical records and health data collected, processed, used, and circulated in American society at the moment - basically the past decade - when automation first began to spread through the health care field?
2. What were the rules of law and definitions of citizen rights that were applied to such traditional patterns of medical record keeping, both in theory and in practice?
3. What kinds of disputes over medical data and civil liberties claims were already arising when computerization arrived?

Presenting such baselines is not a simple task. There is no work in existence that describes comprehensively how medical data are generated and used in American society. Nor is the average citizen, or even the average medical professional or legal expert, aware of how widely the individual's medical and health data now circulate from doctors' offices, clinics, and hospitals to the files of insurance companies, health care review committees, employers, educational institutions, the military, the police, credit bureaus, government licensing agencies, research studies and surveys, and a host of other users. Laying out such a map of medical data uses and the citizen rights issues that have been generated by them is therefore our first goal and the topic of the next three chapters.

To most people, "medical record" probably evokes a picture of a folder in a doctor's office or a chart on a clip-board in a hospital. Our common expectation when we visit the doctor is that we will be asked many questions--about childhood diseases and current problems, about the health of our parents and siblings, about our age and weight, about what we eat and how much we smoke and drink. Then we will be poked, tapped, finger-pricked and examined, and the results of all these probings - mental and physical - will be entered into the folder.

Throughout this process, the patient is usually a willing participant. The doctor needs to know, and the patient accepts that need as a vital ingredient of receiving good medical care. The patient has the same general expectations of hospital care, although a lot more people there need to know--nurses and pathologists, surgeons and anesthesiologists, and the admitting clerk who may insist on knowing the mother's maiden name before it will be permitted that the baby be born or the operation performed. But the probing is accepted here, too, as part of the bargain the patient strikes: personal information in exchange for medical care.

If reminded, the patient will also recall that those who pay his medical bills--whether government agencies or private companies--need to know why the patient was in the hospital, and for how long. But the average patient could probably not say with any certainty what other information about him or her is given to insurance payers.

Beyond this direct experience, however, the concept of medical records is likely to be blurred for most patients. They have made no explicit bargain that their medical records will be shared with employers, or welfare agencies, or licensing bureaus, or government departments, or a host of other non-medical agencies. If the bargain is an implicit one, often the patient is an unwitting participant in the transaction.

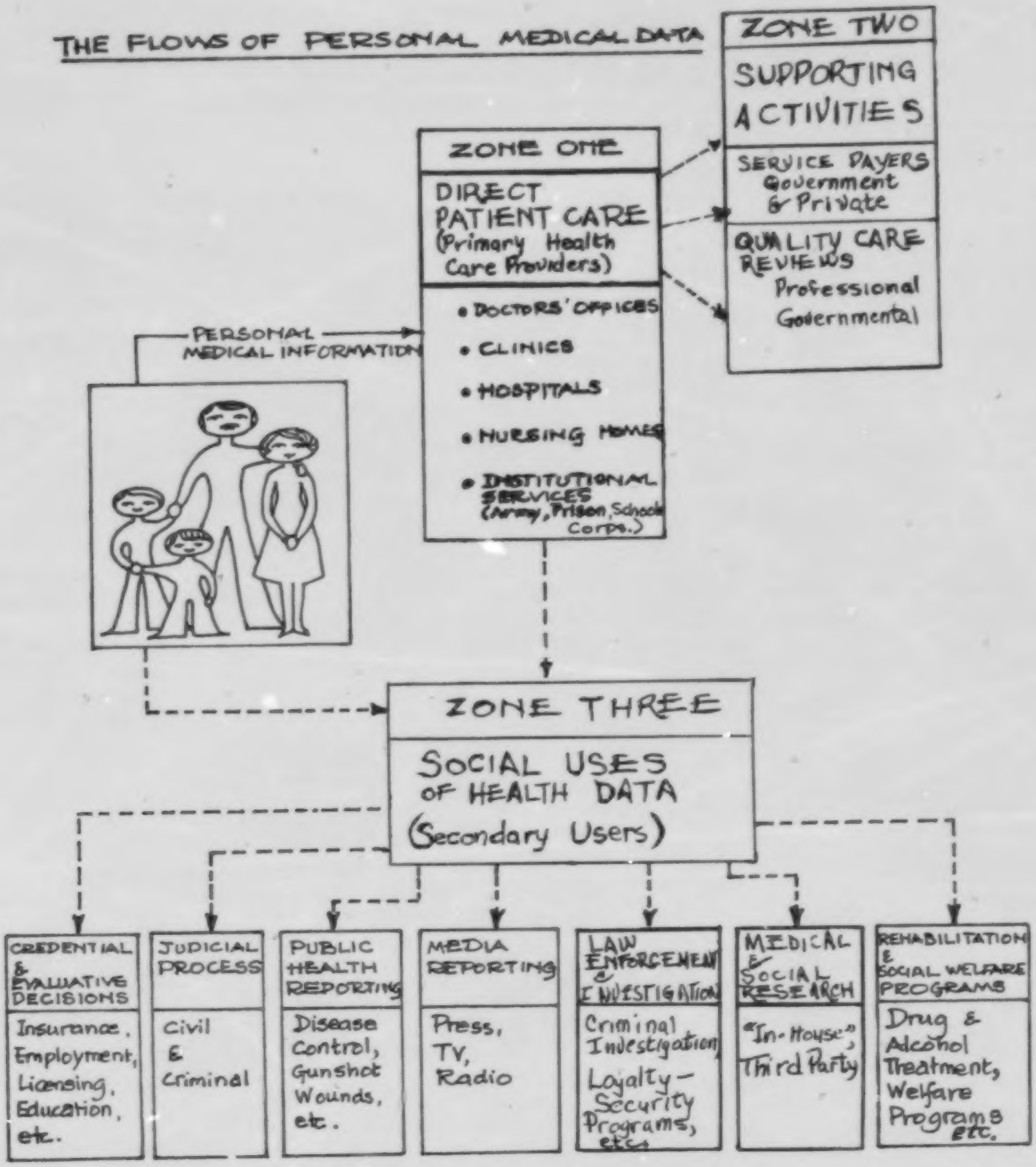
Part I of this study will trace the course of medical records, beginning with the patient's direct encounter with medical care. It will examine who keeps medical records, how they are kept and why they are kept. The various kinds and uses of medical records are divided into three zones, described below. As with any such arbitrary system, some of the items in each of the three zones defy neat labelling; many of them overlap; some are discussed from several points of view. Thus, for example, medical records in law enforcement is discussed in Zone I as part of a physician's duty to report certain conditions to the police, and again in Zone III to describe how law enforcement agencies use medical records. It is hoped that the sense of deja vu will be kept to a minimum, and that where repetition is unavoidable, the reader will be forbearing.

Zone I - Primary Health Care This chapter will describe medical records that are created when a patient seeks health care from a health professional--whether a personal physician, a hospital, a health center or clinic, a college infirmary, a company doctor, etc. It is here that the cycle of medical record-keeping usually begins. And it is here that sensitive ethical and legal questions as to confidentiality and disclosure sometimes pit the medical profession's perceptions of good medical care against the rising consciousness of some patients and consumer groups who seek greater participation in medical decision-making.

Zone II - Service Payers and Health Care Reviewers This chapter will examine the use of medical records by those who pay for medical care--both private insurance companies and government programs such as Medicare and Medicaid. It also surveys voluntary private groups and government agencies that review individual medical records as part of their efforts to analyze the quality of medical care and to determine whether hospitals and other health providers are in fact delivering the health care for which they are being reimbursed. It is especially important to understand the current practices in Zone II, for these two functions--paying for health care and monitoring its quality--prefigure the creation of a universal, pre-paid health insurance program.

Zone III - Secondary Users of Personal Medical Data This chapter will discuss the use of medical records in the non-medical world. From "womb to tomb," - or to put it in medical record terms - from birth certificate to death certificate, medical records are required, among other things, when starting school, going into the armed forces, getting married, travelling abroad, getting a job or a business license, driving a car, applying for life insurance, receiving government benefits, applying for a security clearance, encountering the law, or going on welfare. It is here that breaches of confidentiality and inaccuracies in records can exact a painful human toll.

The chart below diagrams the flow of information just described. The three chapters that follow use the items listed in each Zone as chapter sub-heads.


THE FLOWS OF PERSONAL MEDICAL DATA
ZONE TWO
SUPPORTING ACTIVITIES
SERVICE PAYERS Government & Private
QUALITY CARE REVIEWS Professional Governmental
ZONE ONE
DIRECT PATIENT CARE (Primary Health Care Providers)
• DOCTORS' OFFICES
• CLINICS
• HOSPITALS
• NURSING HOMES
• INSTITUTIONAL SERVICES (Army, Prison, School Corps.)
PERSONAL MEDICAL INFORMATION
ZONE THREE
SOCIAL USES OF HEALTH DATA (Secondary Users)
CREDENTIAL & EVALUATIVE DECISIONS
Insurance, Employment, Licensing, Education, etc.
JUDICIAL PROCESS
Civil & Criminal
PUBLIC HEALTH REPORTING
Disease Control, Gunshot Wounds, etc.
MEDIA REPORTING
Press, TV, Radio
LAW ENFORCEMENT & INVESTIGATION
Criminal Investigation
Loyalty-Security Programs, etc.
MEDICAL & SOCIAL RESEARCH
"In-House", Third Party
REHABILITATION & SOCIAL WELFARE PROGRAMS
Drug & Alcohol Treatment, Welfare Programs etc.

NOTE

Part One draws on memoranda by project consultants Michael A. Baker ("General Patterns of Record-Keeping About People in the Health Care Field: The Pre-Computer Baseline") and George J. Annas ("Judicial Treatment of Medical Records and Confidentiality"). These were produced for the first draft of this report, and are on file with the Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234.

CHAPTER 1. ZONE I - PRIMARY HEALTH CARE

What follows is a description of record-keeping in the private practitioner's office, and then a description of the process in hospitals and other health centers. Record-keeping in which institutions employ health professionals to treat their special populations (e.g., schools, armed forces, prisons) is handled separately, since the existence of a physician-institutional relationship alongside the physician-patient one provides a significantly different setting for viewing ethical and legal problems.

Record Keeping in Physician's Offices

An estimated 80% of health care is delivered by more than 190,000 private practitioners in their offices, with over 900 million patient visits to physicians' offices in 1973.[1] The most important use of the patient's medical record here is as an aid in diagnosis and treatment, with the private physician free to choose whatever form of record-keeping he/she wishes. The broad variety of record-keeping practices to be found in private offices reflects differing medical philosophies as well as the demands of different kinds of medical practice.

Some physicians use their office records only to jog their memories about the social and medical characteristics of patients; they provide care for the most part on the basis of the patients' verbal reports of symptoms and their own most recent tests and observations.[2]

Some physicians, specialists for instance, see thousands of different patients a year; their record of each patient is likely to be very detailed as to diagnosis and treatment, but narrowly focussed on the specific problems referred to them. Participation in group practice also affects the character of a physician's records, since there is apt to be greater demand for communication from other physicians in the group responsible for the patient's care.

Psychiatrists, psychologists and psychotherapists in private practice vary widely in the amount of detail they record on their patients. Psychiatrists are MDs, and they often keep records of their patients' physical ailments, especially where psychosomatic problems are being treated. Some therapists tape-record their sessions; others keep but a few notes in a short-hand only they can decipher. Professor Ralph Slovenko notes that "It is customary to keep records of appointments and billings, but most psychoanalysts and analytically-oriented psychotherapists make no records or notes of patient communications."[3] Of those who do, many store such records under code names or numbers.

Beyond the physician's personal choice of record-keeping methods, there are several other factors that influence these activities:

1. Third-party payers More than 150 million people are protected by regular medical expense insurance, which provides benefits toward physicians' fees for non-surgical care given in the hospital, home or doctor's office.[4] The information that doctors must submit to insurance companies to justify payment for

---

[1] Raised figures indicate the footnotes located at the end of the chapter.

such office visits frequently requires making additional entries into the patient's record.

2. Public Reporting Requirements State statutes require a broad variety of reporting by physicians to appropriate government agencies. Among these are communicable diseases such as TB, venereal disease, meningitis, polio, etc; wounds deliberately inflicted with a deadly weapon; child abuse and neglect; all deaths that are not "natural", as by drowning, from falls, or sudden deaths; and industrial accidents. In addition, physicians must keep a record of their prescriptions for narcotics and other dangerous drugs in a special register which is open for inspection by federal and state authorities.[5]

It is difficult to tell how strictly these reporting statutes are enforced. In a study of 237 private physicians conducted by Consultant Magazine in 1972, it was found that while 60% of those responding felt that venereal disease reporting should be compulsory, in fact only 11% of the physicians reported gonorrhea and only 20% reported syphilis.[6]

3. Malpractice claims About 60% of the malpractice claims made in 1970 were against physicians in private practice.[7] There has been much professional discussion of the sharp increase in malpractice suits, and physicians are increasingly aware that their office records are a prime source of information about the quality of their care. As a result, physicians, like hospitals, are increasingly engaging in "defensive medicine," that is, the ordering of tests and consultations so that the record will show the physician took every reasonable precaution. While it is difficult to estimate the amount of defensive medicine that takes place, some authorities claim that it has at least one beneficial effect: the overhanging threat of litigation does seem to encourage more methodical record-keeping.

Hospital Record Keeping

Thirty million patients are admitted each year to the 900 proprietary, 3,500 voluntary and 2,700 governmental hospitals which offer care for acute conditions.[8] The medical records of these patients may include: identifying information, x-rays, EKG and lab test results, daily observations by nurses, physical examination results, diagnoses, drug and treatment orders, progress notes and post-operative reports from physicians, medical history secured from the patient, consent forms authorizing treatment or the release of information, summaries from the medical records of other institutions, and copies of forms shared with outside institutions for insurance purposes. In some cases, ad hoc staff comments about the patient's character or demeanor are also put in the record.[9]

Hospital medical records vary considerably, so it is difficult to describe the "typical" record. In some institutions, one could find all of the above information in the patient's medical "jacket" or central file, and this could total 80 or 100 or even 150 pages. In others, only the patient's current condition is described in the medical record, but other information is developed in the files of the collection department or the social service department.

In most hospitals, each of several departments--pharmacy, social service, billing--maintains its own files, duplicating most of the information stored in the patient's central record. Often the lines between social service, medical and administrative records are blurred. The "medical" record may contain information about the patient's insurance; the social service file will certainly contain some reference to the patient's medical condition; identification files or the daily bed census reports indicate the ward to which the patient was admitted, such as obstetrics or psychiatry.[10] The patient's hospital record, then, is really several different overlapping files, often kept in separate places.

In many hospitals, there are central medical records handled by medical record administrators, a paramedical profession developed over the last fifty years along with the increase in size of general hospitals and the specialization of the staff within them. More than 11,000 medical record administrators and technicians now work full time at supervising the filing of medical records, enforcing hospital rules about their content and accuracy, and extracting information from them for insurance and other purposes. About 25% of these persons are certified by the American Medical Record Association.[11]

Problems of patient identification and record retrieval are chronic in many hospitals. Some hospitals use a "serial" numbering system in which a new number is assigned to the patient at the beginning of each hospital stay. If the patient returns to the hospital, he or she has to be matched accurately with past records or these cannot be used. A related problem is that the information in the patient's record is often poorly organized. A typical complaint from physicians is that needed information from a thick patient file cannot be easily extracted. As a result, even when the patient's past file can be retrieved, the information recorded in it is often not used.[12]

Unlike the private practitioner's records, hospital records are subject to both internal and outside review. Where federal money is disbursed for health care, such as in Medicaid or Medicare, federal regulations require the establishment of Professional Standards Review Organizations (PSRO) to determine that facilities and professional services are not being misused. Medical records play a central role in such utilization reviews.[13]

The Joint Commission on Hospital Accreditation, a private organization that sets standards for hospital accreditation requires that standard nomenclature be used in diagnoses and that records contain "...sufficient information to justify the diagnosis and warrant the treatment and end results."[14] When the accreditation surveyor reviews hospital facilities and procedures, a considerable part of his or her time is spent on patient records.

Local and state agencies also conduct hospital reviews. Recently, the New York City Health Department condemned three voluntary hospitals participating in the Ghetto Medicine Program for failing to maintain "drug reaction" files necessary to prevent a patient from being injured by a bad combination of medication or by drugs to which he or she had had an adverse reaction in the past.[15]

But poor public hospitals are not the only ones with record-keeping problems. For many hospitals, the Joint Commission's criteria are never entirely achieved. Among the facts of everyday life in hospitals are physicians' tardiness in signing drug orders and completing discharge summaries, and hospitals that ignore some record-keeping requirements because of lack of staff and mounting costs.[16]

In short, hospitals tend to allocate their limited resources to record-keeping tasks that meet immediate needs: to provide minimum information for patient care; to file insurance claims quickly so that the hospital gets reimbursed; to respond to an ultimatum from the Joint Commission on Accreditation that particular record-keeping deficiencies will no longer be tolerated.

Like private practitioner's records, hospital records are used for insurance, both private and governmental, and as protection against malpractice claims. Hospitals are also subject to the same public reporting requirements as private physicians: communicable disease, law enforcement, child abuse, narcotics prescriptions and death certificates.[17] One widely used record is the birth certificate, and the duty to report births falls largely on hospitals.

Birth records serve both research and legal functions, and for Americans, are the closest this country comes to an official identity card: a birth certificate is usually required upon entering elementary school, getting a work permit or driver's license, a passport, entering the armed forces and securing social security benefits. Law enforcement agencies also regard tight birth certification procedures as important. The Immigration and Naturalization Service, for example, uses the birth registration system as one way to stem the flow of illegal aliens.

The U.S. Standard Certificate of Live Birth contains spaces for the names and addresses of the parents, the child's name, the date, and the signatures of a physician or other witness and the local registrar of records. This part of the Birth Certificate is a matter of public record in many states.[18]

The form also includes information about the condition of the mother prior to childbirth, complications which developed during delivery, and congenital or other physical problems the child was observed to have at birth. There is also a space for hospital personnel to note whether or not the child is legitimate. It is not always clear how this decision is made. In an informal investigation of this question, Professor Michael Baker's students found that sometimes it was made by doctors, sometimes by nurses. The patient was not always believed, and the nursing staff would sometimes check "out of wedlock" even when she claimed to be married.

But in large anonymous institutions where a woman may identify herself and the father as she pleases, an illegitimate birth may be recorded as legitimate.[19]

Psychiatric Hospital Records

The medical portion of general hospital records may contain data that relates only to the illnesses being treated. But psychiatric hospital records are likely to be all-inclusive.[20] As sociologists Kai Erikson and Daniel Gilberton put it:

> "The presumption in psychiatric facilities...is that there are no areas in the patient's life (and for that matter, no areas in the lives of his associates) that lie beyond the legitimate interest of the institution. In this sense, the psychiatric dossier is not a brief inventory of selected information; it is a biography, a digest of one person's character and prospects..."

Erikson and Gilberton go on to note that while the record is all-inclusive in one sense, it is highly selective in the sense that only those items that identify the patient as being ill are likely to be included. Thus, if the patient tells a psychiatrist of (a) his bedwetting, (b) of his fear of a teacher, (c) of enjoying family picnics, (d) of his impulse to hit his sister with a hammer, (e) of winning a spelling bee, (f) his terrible dreams, (g) his friendship with an unremarkable boy, (h) his parents' arguments, and (i) his exploits as a young athlete--items (a), (b), (d), (f) and (h) will no doubt be noted in his record; items (c), (e), (g) and (i) will likely be omitted as irrelevant.

Many staff members may contribute to the patient's record--"physicians... psychologists, social workers, nurses, occupational therapists, aides, clerks..." The daily nursing notes may contain comments on the patient's mood, fantasies, plans for the future, emotional outbursts, posture, and interaction with other patients and staff.

In some psychiatric hospitals, patient records are kept in two different categories: material like case histories and certain test results are stored in the central record room or in a locked closet off the ward, while day-to-day operating files such as medication records, nursing notes and doctors orders are kept in the ward where the patient is receiving treatment. The distribution of these records can be a delicate matter. On the one hand, the patient's privacy is best protected by keeping sensitive material off the ward, where students, aides and even charwomen roam largely at will. On the other hand, partitioning of records has the obvious effect of drawing status lines through the hospital staff in a manner that does not serve to improve tempers or the treatment offered the patient. There are hospitals, for example, where nurses do not have access to the more sensitive records, and are dependent on physicians for the most basic information.

The amount of detail in the "typical" patient record varies considerably among psychiatric institutions, especially between those which provide active therapy and the many long-term institutions that are largely custodial. Erikson and Gilberton suggest that in either case, most of the material placed in the file is not read by the people to whom it is addressed; when the records are stuffed with nursing reports and social work interviews, clinicians do not have sufficient time to review them.

Nursing Home Records

The recent scandals involving nursing homes licensed by the State of New York revealed financial exploitation of the inmates, abysmal physical conditions, inadequate nutrition, and a denial of medical care to patients suffering from illnesses. One of the charges made was that patients' records were falsified to conceal stripping the patients of their financial resouces, and to create the impression that patients were receiving care that would make the owners of the homes eligible for state and federal reimbursements.[21]

In a study of a private nursing home in Washington, D.C., where the majority of patients were referred by St. Elizabeth's Hospital, it was discovered that patients were being forced to work fifty to sixty hours a week in the home's kitchen and laundry, or were being hired out to neighborhood businesses for as little as $2.50 a week; that the records were falsified to show that they were not working; or to show visits to doctors or hospitals that never took place; or to show assignments to rooms of one or two inmates, when in fact all the rooms were shared by four people or more.[22]

In 1974, HEW set new standards for nursing home care, including medical care, staff-patient ratios, nutrition, minimum space per patient, etc.[23] The regulations include a Nursing Home Patients' statement of rights, and among the rights guaranteed is "confidential treatment of (the patient's) personal and medical records" and the right to "approve or refuse their release to any individual outside the facility except in case of his transfer to another health care institution, or as required by law or third-party payment contract."

The record-keeping problems in many nursing homes do not usually involve breaches of confidentiality. The more frequent complaint is lack of supervision of the institution. The main emphasis of the new HEW regulations is setting standards for care and monitoring exploitation of the patients.

Records in Other Health Care Settings

Some public health clinics have as complete information about a patient as the general hospital.[24] Pre-natal clinics, for instance, may do a complete medical work-up. But more often the scope of the records reflects the limited medical care provided--vaccinations, treatment for minor illnesses and injuries, etc. Where V.D. treatment or birth control information is provided, the records generated, while similarly narrow in scope, may be extremely sensitive.

Dentists usually keep little information beyond a history of the work performed and x-rays. These are sometimes used as identification for disaster victims and in criminal cases. Dental surgeons maintain a greater range of patient data because they often administer anesthetics and prescribe medications.[25]

Optometrists and podiatrists keep only the patient data relevant to their specific tasks.[26] Local pharmacists can get a pretty clear picture of their customer's medical problems from the medications prescribed and the specialties of the physicians writing the prescriptions. In most pharmacies, prescriptions are filed in sequence, each under a different number. By law, prescriptions for narcotics are filed separately and the pharmacist must account for his supply of narcotics.[27] In many states, the funeral director has access to medical information because he is responsible for filling in identification information and getting the physician to record the cause of death.[28]

Citizen Rights Issues and the Law

1. Privacy

The information gathering process in a hospital is just one factor out of many which tends to strip patients, both figuratively and literally.[29] A patient is constantly being physically exposed during medical examinations, by the backless hospital gown, by the performance of bodily functions in front of ward-mates and staff; by the invasion of the ward by other patients' visitors, gray ladies, clergy, administrative workers, nurses' aides, cleaning people and others whose comings and goings the patient cannot control. Whether a particular hospital staff treats its patients with tact and sensitivity, or with indifference or callousness, the stripping away of the patient's reserve is a dominant theme of hospital life. The hospital staff may view this process matter-of-factly; the patients may not, as the remarks of one patient illustrate:

> "I saw what happened to one of my roommates...She had plastic surgery of the vagina and it seemed like every new nurse and everybody on duty wanted to see...It seemed like just a case of out-and-out curiosity...She was feeling very sensitive and not really wanting to advertise the fact. And now everybody in the world is going to look..."

A hospital, then, is not a place likely to foster an atmosphere of patient privacy, and the collection of intimate medical information must be seen in this context.

Within the hospital framework, it is almost universally accepted that full disclosure by the patient to the health care provider is necessary, often crucial for accurate diagnosis and effective treatment, and few objections are raised about the circulation of patient information among medical personnel *directly* involved in patient care.

However, two questions closely related to privacy sometimes do arise. That is, what should be *recorded* and *how long* it should be kept. One such case involved several San Francisco women who sought to have hospitals return "psychiatric need" letters written by their doctors to justify abortions.[30] Before the 1972 Supreme Court ruling that women have a constitutional right to an abortion, the only way they could secure them in many states was to claim a psychiatric condition that would be exacerbated by pregnancy. Many doctors exaggerated the emotional distress felt by a pregnant patient to justify an abortion in a particular state or for a particular hospital review committee.

A San Francisco woman had secured two abortions at a Kaiser-Permanente facility, one of which had required an "emotional distress" letter. She told the Kaiser authorities that she wanted it back, with no copy kept by the hospital, because if she applied for life insurance, certain government jobs, licensing, etc., she would have to sign releases waiving confidentiality of her records and she could be harmed by the presence of that letter in her file.[31]

Neither she nor any of the other women succeeded in getting the stigmatizing letters back. One hospital justified itself by citing a seven year retention-of-records law. Another said it had to keep them in case of legal actions that might somehow involve the abortion procedure. Another said it would be willing to destroy the letter but would not give the patient the original. As more and more permanent files are created, the question will arise with increasing frequency: When can patients have records that are alleged to be inaccurate, incomplete, biased or based on outmoded social or ethical standards expunged from their files, and by what procedures?

2. *Confidentiality*

The doctrine of confidentiality has its roots in earliest medicine. It was promulgated to reassure the patient that the information volunteered would go no further than the health professional to whom it was confided. The Hippocratic Oath first set out the duty of confidentiality as follows:

> "Whatsoever things I see or hear concerning the life of man, in any attendance on the sick or even apart therefrom which ought not to be noised about, I will keep silent thereon, counting such things to be professional secrets."

The modern interpretation of this oath is contained in the American Medical Association's Principles of Ethics:

> "A physician may not reveal the confidences entrusted to him in the course of medical attendance, or the deficiencies he may observe in the character of patients, unless he is required to do so by law or unless it becomes necessary in order to protect the welfare of the individual or the community."

The relationship of candid disclosure to confidentiality has been set forth in a recent judicial opinion as follows:

> "Since the layman is unfamiliar with the road to recovery, he cannot sift the circumstances of his life and habits to determine what is information pertinent to his health.
>
> "As a consequence, he must disclose all information in his consultation with his doctor - even that which is embarrassing, disgraceful or incriminating. To promote full disclosure, the medical profession extends the promise of secrecy...The candor which this promise elicits is necessary to the effective pursuit of health; there can be no reticence, no reservation, no reluctance when patients discuss their problems with their doctors."[32]

Thus the need to maintain confidentiality is widely recognized as an ethical obligation, as part of the implied contract in the doctor-patient relationship.

The patient's right to confidentiality is popularly portrayed as being solidly entrenched. Medical dramas on television often stress the inviolability of the patient's confidences to the doctor. In police-courtroom dramas like "Perry Mason," only the medical examiner, a public official, testifies on medical matters; private physicians, hardly ever. In soap operas, in which the major action shuttles between the operating room and the courtroom, physicians are often shown agonizing because they are forbidden by medical ethics to reveal some crucial fact which would prevent a miscarriage of justice.

But in real life, the doctrine of confidentiality of medical records often is forced to give way to other public interests--medical, legal or social. In balancing confidentiality against these competing or conflicting interests, confidentiality under American law does not begin with an inherent Constitutional primacy. Free speech, by contrast, is specifically protected by the Constitution, and courts have ruled that it cannot be abrogated except for some "compelling governmental necessity," with the burden on the government to prove that its "necessity" is indeed "compelling."

Physician-patient confidentiality enjoys no such sweeping protection. Thirty-eight states have laws that "privilege" the patient's communication to the physicians, but these laws have many exceptions and "waiver" provisions.[33] A brief explenation of the doctrine of privilege may be helpful to understanding what aspects of confidentiality these laws do and do not protect.

A communication is said to be privileged if the person to whom the information is given is forbidden by law from disclosing the information in a courtroom without the consent of the person who provided it. So privilege applies only to judicial proceedings; it is a legal rule of evidence. Also the privilege belongs only to the patient, not to the physician or other health-care provider.

Unlike the attorney-client privilege, the physician-patient privilege is not recognized in the common law (those laws made by judicial decisions and not by legislative enactment of statutes). It therefore exists only in those 38 states which have passed a statute establishing it.

Perhaps the best way of understanding the limitations of the physician-patient privilege is to list some of the circumstances under which physicians or other health professionals are (a) permitted to reveal medical information about their patients; or (b) affirmatively required to reveal such information:

A. Public Reporting Laws: Almost all states have laws requiring physicians to report a wide variety of conditions to public authorities.[34] There are four categories of reporting statutes:

(I) Birth and death certificates. As already noted, the birth form calls for considerable information about the parents. Some states also require the filing of a certificate for a fetal "birth" either by miscarriage or abortion. One such statute was recently declared unconstitutional in New York, as an invasion of privacy.

If death is accidental or sudden, or if foul play is suspected, the medical examiner or coroner is required to do an autopsy and file a report of his findings with the district attorney. These reporting statutes are almost universally complied with, and failure to do so is generally a misdemeanor punishable by both fine and imprisonment.

(II) Infectious, contagious or communicable diseases. The California statute, for example, lists: "Cholera, plague, yellow fever, malaria, leprosy, diphtheria, scarlet fever, smallpox, typhus, typhoid, paratyphoid, anthrax, glanders meningitis, tuberculosis, pneumonia, dysentery, erysipelas, hookworm, trachoma, dengue, tetanus, measles, German measles, chickenpox, whooping cough, mumps, pellagra, beriberi, Rocky Mountain spotted fever, syphilis, gonococcus, rabies or poliomyelitis." In addition, the California statute requires reporting to the Motor Vehicle Bureau of any disease that might cause "lapse of consciousness" (e.g. epilepsy).

(III) Child abuse. Reporting generally comes from the emergency rooms of large city hospitals. Some states have passed legislation to set up registries of potential child abusers in order to systematize reporting.

(IV) Wound Reports. "Bullet wound, gunshot wound, powder burn, or any other injury arising from or caused by the discharge of a gun or firearm, and every case of a wound which is likely to...result in death and is actually or apparently inflicted by a knife, icepick or other sharp or pointed instrument."

These reporting statutes are examples of how legislatures have specifically codified exceptions to the physician-patient privilege. A physician could probably also notify a non-government agency, such as an airline, that a patient-pilot had experienced blackouts under the same theory. The reason for this exception is that at some point, the competing interests of society outweigh both society's and the individual's interests in maintaining medical confidentiality.

B. Consent of the Patient: If a patient brings a lawsuit against a physician or hospital for malpractice, he/she will probably want to bring his/her medical records into court to support the claim for damages.[35] The patient may wish to bring medical records into court when suing a third party for damages in a personal injury case to document the extent of the injuries suffered. No breach of confidentiality is involved in such cases, since the "privilege" belongs to the patient. In one case, for example, a psychiatrist who attempted to assert the physician-patient privilege over the objections of his patient, to protect the patient's best interest and safeguard psychiatric privacy in general was sent to jail in California for contempt of court.[36]

Often, the patient's consent to release medical information is not at all clear-cut.

(I) "Implied Consent". In many hospitals, people not involved in the patient's care may have access to the patient's record, including nurses on all three shifts, medical students, interns and residents, financial workers, ward secretaries, social workers and researchers of many kinds. All of this takes place on the "implied consent" of the patient - that is, his/her very presence in the hospital is taken to imply consent for widespread in-house access; this usually occurs without the patient being aware of it.[37]

(II) General or "Blanket" Consent. Upon entering a hospital, a patient may be asked to sign an authorization which says essentially that the hospital may release medical information about the patient to anyone it thinks should have it.[38] This will include private or government insurance payers, utilization review committees, and others monitoring the quality of patient care or cost. Thus, the need to assure payment for medical care and to assure the quality of that care take precedence over the doctrine of confidentiality. Generally, no restriction is placed on the amount or the relevance of the material that may be released or the use which many of these third parties may make of this information.

(III) Partial Consent. Situations often arise in which some courts have found that the patient has "waived" his right to confidentiality. In one case, a civilian employee of the Air Force asked his doctor to make a partial disclosure of his medical record to his employer to explain his absenteeism.[39] The court held that because of this consent to disclose part of the record, the patient was "estopped" from complaining when his physician made full disclosure, including his alcoholism.

In another case, a court held that an application for life insurance was a waiver of confidentiality.[40] In this case, the pediatrician of an infant informed a life insurance company of a congenital heart defect of which he had not informed the child's parents.

(IV)Consent for Minors. Special problems are involved with health care for minors. Generally, parental consent is required for both the treatment of a minor and for the release of the child's medical records. However 49 states (the exception is Wisconsin) now allow minor youths to receive venereal disease treatment without the consent of their parents and in strict confidentiality. Many states have also lowered the age of consent either for all health care or for specific categories of treatment, such as pregnancy and pregnancy prevention.*

C. Best Interests of the Patient: Some state laws make an exception to the physician-patient privilege to permit disclosure to third parties in "the best interests of the patient." The New Jersey Statute, for example, states that:

> "[N]othing in this section shall preclude disclosure upon proper inquiry, of information as to a patient's current medical condition to any relative or friend...if it appears that the information is to be used directly or indirectly for the benefit of the patient."[41]

Courts, too, will give physicians wide latitude in making disclosures that physicians believe are in their patients' best interests. A court found it permissible for a mental institution to which parents had taken their child for help to report to her school that she was "feeble-minded" and to predict that "at the time she is about sixteen, she should have progressed to about the fourth grade level."[42] Although there has been little judicial explication of this exception, one can deduce that telling a spouse of a patient's heart condition, or telling an employer of a roofer that the roofer is subject to blackouts and would be endangering his life in this trade, would probably qualify.

---

* Adele D. Hofmann, M.D., "Confidentiality and the Health Care Records of Children and Minor Youth," Paper prepared for Conference on the Confidentiality of Health Records, Key Biscayne, Florida, November 6-9, 1974, p.5.

D. Supervening Interests of Society: The leading case here is Simonsen v. Swenson, decided by the Nebraska Supreme Court in 1920.[43] A man who was visiting a small town was seen by a physician, who was also the physician for the hotel where the patient was staying. The physician diagnosed syphilis and advised the patient to "get out of town" or he would tell the hotel. When the patient refused to leave, the doctor notified the landlady who disinfected his room and put his belongings in the hall. The court decided that the doctor had the right to reveal as much information about a contagious disease as was necessary for others to take precautions against becoming infected, and that his actions were justified.

In a lawsuit filed in 1974, a doctor informed his patient's fiancé that she had syphilis, and as a result, the wedding was cancelled.[44] In this case, however, the doctor had misread the premarital blood test, and the patient is suing him for $500,000.

The California Supreme Court has recently extended the "supervening interests of society" exception to the psychotherapist whose patient threatens bodily harm to a named individual.[45] The court went one step further, however, in finding an affirmative duty on the part of the therapist to warn the named "victim."

E. The Public's Right to Know: This exception applies mainly to the press, and press interest in medical records is usually related to individuals who are newsworthy, either because of their prominence (actor, politician, sports figure) or because they are part of a current story (accused criminal, birth of quintuplets). Generally, hospitals will give out only minimal information about a patient's condition unless they have express permission from the patient to release more, as when a politician authorizes the release of detailed information to avoid damaging public speculation. Police spokesmen sometimes release information about criminal suspects against their wishes.

Two leading legal commentators, J.R. Waltz and F.E. Inbau, writing in 1971, argue that:

> "The fact that the patient is not a 'private' person but rather a celebrity who customarily feeds on publicity...will probably be considered of no consequence where intimate medical data, covered by explicit legal and ethical requirements of confidentiality are involved. The fact that medical data are newsworthy or will advance science is likewise not controlling."[46]

The authors state that one exception to this might be the condition of the President since the public has a right to this information. After the hospitalization of former Presidents Truman, Eisenhower and Nixon, one might include former presidents in this category, although public interest in their conditions was certainly not as great as when they held office.

A separate question is raised by the release of medical information obtained in a questionable or illegal manner, as in the case of Senator Thomas Eagleton and more recently, Manhattan District Attorney Frank Hogan.[47] The New York Post revealed that Hogan, up for re-election, had been hospitalized for a stroke and lung cancer, although his office said it was for fatigue. The Post quoted directly from medical reports to support their claim, and defended the use of stolen hospital records by saying the electorate had a right to know the facts.

In answer to the question: Does it matter how the press obtains private medical information? - the case law seems to indicate that so long as the press did not themselves commit a crime in obtaining the information, they can publish it with impunity if there is a legitimate public interest in it. The press will not be held as accessories for receiving stolen goods because the courts will generally find that what they received was "information," the actual documents having been copied and replaced.

F. The Judicial Process: As noted, in the absence of a state statute, the courts do not recognize a physician-patient privilege. The common law principle is that the courtroom is an arena for discovery of the truth, and confidential communications should not be beyond the court's reach. The late Dean Wigmore, perhaps the leading legal expert on evidence, argued that the privilege frustrated justice by denying truthful information to the courts; that most information communicated to a physician is not intended to be held strictly confidential since most of one's ailments are both apparent and openly discussed; and that even if it were meant to be confidential, it would be disclosed to the physician even if no privilege existed.[48]

Retention of the privilege was the most controversial item in the new Federal Rules of Evidence which became law in 1975. Initial versions eliminated the privilege entirely. The final version provides that the privilege shall "be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience." Where, however, state law governs a case, the privilege shall be "determined in accordance with state law."[49] A special privilege was retained, however, for communications between psychotherapist and patient.

Where courts have found a breach of patient confidentiality, the cases have generally not turned on that breach alone. The key element has usually been publication, generally accompanied by a photograph of the patient, that could be construed as commercial exploitation or advertising. In such cases, sometimes the suit is against the publisher, and not the physician or other health care provider. Some illustrations:

In 1939, Time Magazine published the story of a young woman receiving treatment for uncontrollable gluttony. She sued the magazine and was awarded $1,500.[50] A hospital was sued for permitting newspaper publication of an infant born with the heart outside the body.[51] A newspaper syndicate was sued for publication of an x-ray disclosing a hemostat that had been in the patient's abdomen for four years.[52] Physicians were sued for filming a Caesarean section and using the film as part of a documentary.[53] A medical journal was sued for publishing a physician's "before and after" pictures to illustrate treatment of "saddle nose".[54]

Other cases indicate that publication is not always necessary. In Horne v. Patton for example, a case involving disclosure of medical information to a patient's employer, an Alabama court in 1973 found that: "unauthorized disclosure of intimate details of a patient's health may amount to unwarranted publicization of one's private affairs...such as to cause outrage, mental suffering, shame or humiliation to a person of ordinary sensibilities."[55]

Any discussion of the law and confidentiality must recognize that the law is very sparse. In the first place, few patients bring such lawsuits because they usually have no way of knowing who has had access to their records and for what purpose. Even when patients learn of breaches of confidentiality, they may decide they cannot afford the time or money for litigation. Most important, a lawsuit means a public trial which only serves to publish the very information they wish to remain confidential.

A further deterrent is that the prospects of such litigation are not encouraging. While patients may sue for invasion of privacy or breach of confidentiality, or for defamation if the information released about them is false, the fact is that there is no reported U.S. case in which a physician or hospital has ever had to pay money damages for breach of confidentiality.[56] (As noted earlier, some publications have paid damages.)

Eliminating Exceptions by Statute:

One way to increase the confidentiality of medical records is to protect them specifically by statute. An example is the New York statute drafted by Professor William J. Curran to protect the Multi-State Information System for Psychiatric Patient Records.[57] The statute specifically declares that these records are "confidential and not subject to examination in the courts or by agencies of this state...(and) are not public records...and not subject to subpoena in any court or before any tribunal or administrative agency."

On the Federal level, the Comprehensive Drug Abuse Prevention and Control Act of 1970 provides that:

> "The Secretary (of HEW) may authorize persons engaged in research on the use and effect of drugs to protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons so authorized to protect the privacy of such individuals may not be compelled in any Federal, State or local civil, criminal, administrative, legislative or other proceedings to identify such individuals." 58

In the case of People vs. Newman in 1973, New York's highest court reversed a lower court ruling that the Director of a Methadone Clinic, protected by the Federal statute, had to turn over photographs of black male patients between the ages of 21 and 35 to the police.[59] The case arose when the witness to a killing told police she believed she had previously seen the killer in the waiting room of the clinic.

Thus, a properly drafted statute can eliminate some of the exceptions to the doctrines of privilege and confidentiality.

3. Patient Access to Medical Records

The movement to promote policies and laws to give patients access to their medical records parallels attempts by parents and students to get access to school records and of consumers to get access to credit bureau records. All of these are part of a growing citizen movement to affirm individual self-determination and to place limits on the power of institutions to determine important aspects of people's lives without due process oriented procedures.

As to medical records, when these were in fact used only by the physician or the hospital, it may have been only curiosity when patients asked to know their contents. But now that medical records are widely shared with health insurance companies, government payers, law enforcement agencies, welfare departments, schools, researchers, credit grantors, and employers, it is often crucial for the patient to know what is being recorded, and to correct inaccuracies that may affect education, career advancement or government benefits.

This drive for patient access runs head-on into the traditional view of health professionals that they alone should decide what patients should know about their records, that access might lead patients to become confused or anxious, and that this undermines good medical care. While there are a few dissenters in the medical profession who believe that patient access to medical records is good medicine, the overwhelming majority of health professionals still oppose it. The position of the American Medical Association summarizes the main professional view:

> "It is our position that the right of a patient to medical information from his physician is based upon the fiduciary relationship which imposes a duty to act in the best interest of the patient. It would be a violation of that duty to provide information which would be harmful to the best interest of the patient as a matter of sound medical judgment. It is our position that a physician has both a right and a duty to withhold information in circumstances in which he reasonably determines that it would not be in the best interest of the patient."[60]

Between the adamant position of most physicians and the equally adamant position of consumer advocates is a compromise position which calls for partial access. Dr. Simon Auster, Director of the Fairfax-Falls Church Mental Health Service Board, commenting on a proposed Virginia access-confidentiality statute, suggests that patients be given access to any part of their record that may be disseminated to others so that patients would have "an opportunity in advance to confirm its accuracy or to prevent its release." At the same time, he would keep from the patient those parts of the record that reflect the physician's "thinking out loud" or subjective impressions.[61]

Overview of the Law on Access:

A few states have special access statutes which enable patients treated in hospitals to view and copy their medical records. (Some statutes limit this right to the patient's attorney or authorized representative.) Perhaps the most liberal of these is the Massachusetts statute which gives patients an absolute right of access both during their hospital stay and after discharge.[62]

The Massachusetts statute, enacted in 1945, was sponsored by Edward R. Butterworth, an attorney, who had difficulty getting hospital records for clients involved in cases in which the records were needed. Mr. Butterworth, however, has recently been forced to sue a hospital that refused to release patient records even in the face of the statute. His experience is not unique. A 1973 study of the effect of this statute in the Boston area by the Center for Law and Health Sciences of Boston University Law School revealed that 9 out of 10 major hospitals denied patient requests for information.[63] Only one followed the statutory language. A typical response came from the Director of Boston's Beth Israel Hospital: "We would prefer to send the chart to a physician so that he or she might interpret the information to the patient... in order to make a reasonable judgment on the request that the patient directly receive the chart." A 1975 survey by the Massachusetts Public Interest Research Group found that only 3 out of 28 hospitals examined were in compliance with the access law.[64]

Where there is no special access statute, the only way a patient may be certain of obtaining information from his medical record is to file a lawsuit against the doctor or hospital involved (usually alleging malpractice) and obtaining the record through court-sanctioned discovery. This fact was noted by the Secretary's Commission on Medical Malpractice (HEW) in 1973 which found that "the unavailability of medical records without resort to litigation creates needless expense and increases the incidence of unnecessary malpractice litigation."[65]

Health professionals frequently deny patient access to medical records on the ground that they are the property of the physician or hospital. However, the few appellate court decisions have almost uniformly held that while the physician or hospital may own the paper on which the record is written, the interest of the patient in the information is so vital that he does have a right to a copy of it.

In one case where an insurance company sought access with the patient's authorization, the court said the hospital is only the custodian of the record, and the patient has a property right in it sufficient to allow him to copy it without having to sue.[66] A New York Court held that a hospital cannot withhold a patient's medical record for the purpose of concealing the identity of a physician who may have committed malpractice on the patient.[67] In a District of Columbia federal case, a dispensary and a physician were ordered to hand over medical records to a surviving son even though the statute of limitations for a wrongful death action had expired.[68] The Court held: "We are unwilling to hold that one to whom a duty to disclose medical data is already owed is compelled...to engage in legal proceedings to attain a loftier status."

In the area of mental health, however, the case law is not unanimous. In a Texas case, in 1964 a patient was able to obtain access to his mental institution records on the ground that the institution was "public" and the records were open to inspection by patients.[69] A New Jersey court found that the state access statute applied to eight mental patients who desired access to help challenge their involuntary commitments and the quality of the care they received.[70]

But in a recent Federal District case in New York, the court decided against a patient's access on the narrow ground that "neither the statutory, administrative nor decisional law of New York recognizes a former patient's entitlement to his medical files in the absence of pending litigation."[71] The case involved a woman who wanted her records to help her write a book about her experiences. This case is on appeal to the Supreme Court.

Thus, in states with access statutes, patients often must sue to enforce the statute. In states without them, hospital medical records are usually governed by regulations of the state hospital licensing agency. A sample of these regulations indicates that most permit hospitals to adopt restrictive access procedures.[72] While all states permit inspection upon court order, many limit access to the patient's attorney or insurance company. As a practical matter, then, hospitals can control access in most cases in which the patient is not willing to resort to litigation.

The access statutes do not cover private physician's offices, possibly because while legislatures were sure of their power to regulate hospitals, they were uncertain of their power to interfere with a physician's private practice. Civil liberties groups report two instances of unsuccessful attempts by patients to gain access to records held by private physicians: In one, a woman was not able to find out whether an infertility drug given her by a physician 20 years ago was stilbestrol, now suspected of being related to cervical cancer in female offspring.[73] In the second, a woman who recently wrote her doctor asking what medicine she was treated with a few years previously has not been able to obtain this information.[74] The possibility of a malpractice action probably explains the reluctance of the doctors in these cases.

The closest analogy to private physician's records and access is x-rays. In a lower court case, and in an appellate decision, the courts held that the physician owned the x-rays and did not have to grant access to them to the patient.[75]

Legal Trends Toward Greater Patient Access

In the same way that the statutory and case law are reconsidering access in employer-employee relations, police and suspect, seller and buyer, etc., so too is the doctor-patient relationship undergoing change. Before 1960, all a physician needed was sufficient patient consent to protect against an assault and battery action for unauthorized touching. Since that time, state courts have consistently recognized that before giving consent, a patient needs a certain amount of information about his condition, the recommended treatment, and its probable results.[76] The new reasoning here is that the patient has a right to self-determination, a right to refuse or to choose between alternative treatments.

Before 1972, legal commentators felt safe in saying that a physician could be guided by the doctrine that "good medicine is good law."[77] In that year, however, three separate jurisdictions held that doctors could no longer limit their disclosures to what "the average medical practitioner would disclose under similar circumstances."[78] The new test must be based on the *patient's need to know*, that is, whether the patient was told enough about the treatment and its risks (death, disability, recuperation) to decide whether to accept the doctor's recommendation. This duty to disclose, ironically, was based precisely on the "fiduciary nature" of the doctor-patient relationship that the AMA has relied upon to deny patients access to their medical records.[79] These decisions are as yet the rule in only a few states, but they indicate the trend of some courts to view the doctor-patient relationship as a decision-making partnership instead of as a medical monopoly.

While the courts have taken a giant step in recognizing patient autonomy, physicians may still invoke the "therapeutic privilege" to deny access. The general rule stated by the California Supreme Court in *Cobbs* vs. *Grant* is: "A disclosure need not be made...when a doctor can prove...that the disclosure would *so seriously upset the patient* that the patient would not (be) able to dispassionately weigh the risks of refusing to undergo the recommended treatment." (emphasis supplied)[80]

While this tends to limit the doctrine of patient access, it does not put the physician back in ultimate control of patient information. It is now presumed that every adult patient will be fully informed unless--as the court held in Natanson vs. Kline - the physician can prove that "a complete disclosure...could so alarm the patient that it would, in fact, constitute bad medical practice..."[81] In the ordinary case, there would seem to be no warrant for suppressing facts.

While the limits of the "therapeutic privilege" have not been carefully defined, at least one court has recommended that wherever a physician invokes it, he or she should be required to disclose the information to a close relative.[82] The problem with this approach is that it may be used to restrict the competent patient's role in decision-making, treating him as though he were incompetent, even though he is not.

The Federal Privacy Act of 1974 and Its State Counterparts

All of these issues--of privacy, confidentiality and patient access--are being directly affected by passage of legislation controlling the use of information by government agencies as primary health providers. The Federal Privacy Act of 1974 requires federal agencies which maintain identified records on individuals to 1) list those data systems and their purposes in the Federal Register; 2) collect only that information which is necessary for the agency to perform its duties; 3) state the "routine uses" of the data collected, for which it is not necessary to obtain the data subject's permission; 4) obtain the individual's signed consent for all other releases of information; 5) keep a log of all such data exchanges; and 6) provide data subjects with access to their own records and the opportunity to correct inaccuracies.

In addition, seven states have passed similar Fair Information Practices Acts. (They are Minnesota, Utah, Arkansas, New Hampshire, Massachusetts, Ohio, and Virginia.)

MEDICAL RECORDS FOR SPECIAL POPULATIONS

Large groups of people have medical care made available to them because of their special relationship to a particular institution or organization: the armed forces provide medical care for servicemen; correctional institutions provide it for inmates; some industrial corporations provide medical care for employees; and some colleges provide it for students.

Under these circumstances, the health care providers are not usually independent practitioners but employees of the institution. While part of their function is to serve their patients, another part is to advance the goals of the institution. Sometimes this dual loyalty serves both the patient and the institution well; sometimes the conflict in loyalty undermines the doctor-patient relationship and interferes with the delivery of medical care.

What follows is a brief review of some aspects of medical record-keeping practices in correctional institutions, the armed forces, employment and colleges.

Correctional Institutions. What must be emphasized first is that medical care in correctional institutions, like every other aspect of inmate life, is subordinate to security.[83] Almost invariably, security considerations govern where medical care is given, when it is given, and who participates. This means that patient interviews, starting with admissions, are never conducted in private. There are always guards present, and almost always other inmates. At the daily sick call, it is not customary to keep records at all.

Here is a description of daily care at Attica prison, in New York State;

> "Dr. Williams spent most of his time with inmates separated from them by a wire screen. When they lined up for sick call, he and an associate prison doctor, Paul G. Sternberg, were on the other side of a waist-high counter; the screen ran from counter to ceiling. No examinations were given, except in rare cases. The patient described his problem. Through the screen, the doctor gave him medication, often aspirin, sometimes a placebo, not infrequently a tranquilizer if the complaint was psychological. Sometimes one of the doctors would dismiss the complaining inmate since both believed they could tell by looking at a man whether he was malingering." 84

In the District of Columbia jail, the sick call is almost identical with the one described above, except that a pre-screening of inmates who place themselves on sick call is conducted by Medical Assistants, inmates who have already been convicted of crimes and who, ironically, are accorded higher privileges than those awaiting trial.[85] The Medical Assistants make the rounds of the cellblocks and dispense aspirins to those inmates whom they do not consider ill enough to go on sick call. As in the other two institutions, prisoners with medical emergencies are taken to the city hospital for treatment.

Thus, for the great majority of the prison population in these institutions and others like them, there is very little formal medical record-keeping, except for the relatively rare prisoner who is treated in an outside city hospital. Copies of these outside medical records are given to the institution's administrators. Sometimes they are not even given to its medical staff.

The lack of medical records for inmates treated in outside hospitals handicaps the limited medical staff of the prison even further. Dr. John L.S. Holloman recounts the difficulty of dealing with a patient in New York who had been shuffled often between the jail and the county hospital.[86] The inmate was suffering from severe neurological damage. "He has made numerous trips to the hospital facilities. Nevertheless there is no medical information concerning the prisoner available to the medical staff here. To send patients for care and then to fail to keep useful medical records seems to be a waste of effort and money."

According to Arpiar Saunders, Associate Director of the National Prison Project, most medical information about prisoners is placed in their general records by non-medical personnel, primarily guards, but sometimes by prison teachers, social workers or the clerical staff.[87]

If the facility is a detention center rather than a permanent prison, the general record, including medical information, follows the prisoner when and if he is assigned to a permanent institution. Many permanent prisons assign inmates to cellblocks according to the seriousness of the crime, and also according to the evaluations made in the detention center. If the inmate's record shows that he was a "troublemaker," or a homosexual or a malingerer, he may be assigned to an undesirable cellblock, or a segregated cell, or put on "deadlock" (confined to cell with no privileges).

Inmates' records are routinely available to prison personnel. In addition to playing a role in initial cell assignments, they are used by disciplinary boards within the institution and may play a role in determining the severity of punishment for an infraction. They are also used by parole boards, who give considerable weight to derogatory comments by guards when deciding whether or not to grant parole.

Medical Records in the Armed Forces: Military doctors have an affirmative duty to report to the military command any medical information they think relevant to the soldier's performance or status. "Military law, quite simply, does not recognize the physician-patient privilege," according to Captain David B. Knoll of the Judge Advocate General Corps.[88] He goes on to note that "...A military doctor performs examinations as part of his official duties, and information thereby acquired would be official. Maintenance of complete medical records on all persons in the military services is of substantial concern to the services themselves."

The lack of a physician-patient privilege is crucial for members of the armed forces since the medical information they volunteer to military doctors may be used by the command to determine their fitness for promotion, or whether or not they should be summoned before an administrative hearing board or court-martialed. If either of these disciplinary procedures is invoked, military doctors may give evidence at them based upon what the serviceman or woman confided in them.

Where a court-martial is a possibility, military physicians are required to give the patient some form of an "Article 31" warning that what he says may be used against him. The military version of the Fifth Amendment provides: "...no person... may interrogate or request any statement from an accused or a person suspected of an offense without first informing him of the nature of the accusation and advising him that he does not have to make any statement regarding the offense...and that any statement made by him may be used as evidence against him in a trial by court-martial." The military physician, however, does not have to use the formal language of Article 31. It is enough for him to tell the patient that whatever he says during an interview is not privileged.

However, no such warning is necessary unless a court-martial is in the offing, as a recent case demonstrates. A private voluntarily consulted an Army psychiatrist for help about his homosexual feelings.[89] On the following day, the psychiatrist filed a detailed report with the soldier's superiors, and recommended that he be discharged for administrative reasons under the provisions of the regulations regarding homosexuality (undesirable discharge). The recommendation specifically noted that there was no evidence of a mental illness which would necessitate a medical discharge. (A medical discharge entitles a soldier to veterans' benefits.) The soldier describes the consequences of the psychiatrist's recommendation:

> "Discharge proceedings were begun against me and, after being threatened with a court-martial, I signed a statement and waived my right to counsel and a hearing... Shortly thereafter H____ and others told me I had to name names or I would not get out. Under such coercion, I named P______ and then, regretting what I was forced to do, I denied it and all the other admissions as well...
>
> "In the past ten years my undesirable discharge has haunted me... My civil service job application was returned, and Bank of America rejected an application for a Federally Insured Student Loan...The VA also denied me my veterans' benefits. Despite the incidents ten years ago, I repeat, as I did then, that I am not a homosexual..."

As the above case makes clear, medical information not only affects the serviceman or woman's career while in the armed forces, it also affects the kind of discharge he or she receives, which in turn affects the veteran's opportunity for employment and his or her eligibility for veterans' benefits.

Until March, 1974, servicemen and women were given a Separation Program Number on their general or honorable discharge papers which, unbeknownst to the veteran, was a code to employers and others and which frequently signified derogatory information.[90] Many of these numbers were based on medical information or records. Among them:

Codes 249-257 - homosexuality; 261 - Psychiatric or psychoneurotic disorder; 262-263 - bedwetting; 264 - behavior disorders; 274,277,278 - physical disability, not entitled to severance pay; 287 - unclean habits, venereal disease; 288- anti-social behavior; 289 - alcoholism; 361-362 - homosexual tendencies (without overt homosexual acts); 369 - cyclothymic personality (manic-depression); 375 - failure to meet medical fitness standards; 384 - drug abuse; 388 sexual perversions; 41E obesity; 46B, 46D - sexual deviate; 460 - schizoid personality; 480 - personality disorders; 552 - court-martial, homosexual; 651 - physically disqualified.

More than 400,000 Vietnam veterans have been given such derogatory separation numbers. While these secret numbers may frequently adversely affect a veteran's job opportunities, an undesirable or dishonorable discharge is virtually certain to do so. Such discharges are also an outright bar to veterans' benefits in housing, education, pensions, medical care and civil service ratings.

Medical Records in Employment

Although virtually all businesses provide group health insurance coverage to their employees, most corporations limit primary medical care to first aid stations and periodic health screenings. The IBM Company is a good example of a large corporation's occupational health program in which special attention has been given to the rules for information use.

IBM has 250,000 employees, 150,000 of them stationed in the United States. Its domestic medical department employs 120 nurses, 32 full time physicians, 40 part-time specialists, including psychiatrists, and 250 "fee for services" physicians. Its medical facilities handle 650,000 employee visits per year, 150,000 of which involve physician contact.[91]

Between 10% and 20% of all first-aid visits are for occupational injuries; the remainder are for non-occupational illnesses or injuries. In addition to providing treatment for specific complaints, IBM offers a Voluntary Health Screening Examination Program. Approximately 75% of all employees participate in this multiphasic screening system. In the introduction to the pamphlet explaining the Screening Program, employees are told:

> "The program is completely voluntary,and the decision to take part in it is entirely up to you. I also want to emphasize the confidential nature of your examination results which are seen by the professional staff members of the IBM Medical Department, your personal physician if you wish, and no one else. The only instance where health information is obtained during an examination would have to be revealed is when an employee is found to have a suspected communicable disease which must be reported under State law."

The Voluntary Health Screening Examination Program is designed, according to Dr. John Duffy, Director of IBM's Medical Department, "to give the employee advance warning of the most common chronic health problems, as well as to alert the employee to conditions which could cause future health problems. The frequency of medical screenings depends on an individual's age. The older a person becomes, the more often the screenings take place."

All results of tests comprising the Screening Examination are fed into a computer which compares them with the expected statistical profile for the employee's sex and age, and with any earlier Screening Examinations that the employee may have taken. The computer then produces a detailed report of the Screening Examination, making special note of irregularities. The report is then forwarded to the IBM Medical Department where it is inserted into the employee's confidential medical record. If a potential health problem is disclosed by the report, an IBM physician or nurse will suggest that the employee consult his or her personal physician. Upon receiving the consent of the employee, the latter's personal physician will be advised of the results of the screening examination. Dr. Duffy especially notes that "the results of the examination will have no effect whatsoever on the employee's job."

In addition to its express purpose of advising individual employees about their health, the program is designed to furnish statistical data. With the aid of the computer, health examination information is gathered on men and women of widely varying age, geographic location and medical history. The results in summary form enable the IBM Medical Department to develop prognostic techniques. The brochure describing the research aspects of the program points out that:

> "All medical data used in these research studies will be handled in a completely confidential and anonymous manner, and will in no way identify individual participants in the program."

Although the Medical Department does not make medical records available to company managers or supervisors, it does, with the employee's knowledge, inform management when a medical problem is work-related, so that an employee with epilepsy, for example, would not be assigned to handle high-voltage equipment. Approximately 5% of all employees are within the Bureau of Labor Standards definition of handicapped, and 20% are subject to restrictions (epileptic, controlled diabetic, etc.) The same policy is applied to the psychiatric consultation provided. If there is no problem with performance at work, there is no feedback to management. "When illness is impacting job performance or a job is contributing to illness, management is given, on a need-to-know basis, the recommendations which will best serve the needs of the employee and the company."

IBM complies with all State and Federal reporting requirements, including findings of drug abuse among employees and infection with communicable diseases. It complies with the record-keeping requirements of the Occupational Safety and Health Act which requires the maintenance of up-to-date records on occupational injuries and illness to be made available on request to government officials. The company must also furnish appropriate records to the Workmen's Compensation Bureau on request.

In this connection, Dr. Duffy noted that while Social Security numbers are used in filing these Workmen's Compensation reports, IBM uses its own numbering system for internal medical records of its employees.

When IBM Medical Department records are subpoenaed, the company will copy medical department records and send them to the employee's personal physician upon receiving the written consent of the employee.

The range of medical services provided by IBM for its employees is typical of the practices of the big corporations listed in Fortune magazine's Leading 500 Companies. The special policies that IBM has adopted to protect the privacy of employee medical records will be described in the concluding chapter.

Medical Records in Colleges

Many colleges and universities maintain student health services where primary care is provided by physicians and other health professionals employed by the school. (Elementary and secondary schools generally provide only specialized services such as immunizations, eye and hearing tests, etc. and these record-keeping practices are described in Zone III.)

A survey conducted in 1968 of 165 American colleges and universities (and 8 Canadian universities) examined their medical record-keeping practices.[92] While the survey focussed primarily on student psychiatric records, it revealed some general medical record keeping procedures as well.

Virtually all of the school medical directors acknowledged the need for confidentiality of student medical records. As one medical director put it: "If the student body does not know without any doubt that their contacts with the health service will be treated as privileged, then the very effectiveness of this health service is quickly lost." But in spite of the endorsement in principle, the practices among schools varied widely.

1. Informing Parents: The great majority of American schools - 145 in all - responded to the survey by stating that parents are not routinely informed by the health service when the treatment is for short-term illness or on an outpatient basis. Most of the schools, however, do notify parents of hospitalization, serious illness, or a suicide attempt. The eight schools which do not inform parents under any circumstances are all graduate schools where the great majority of students may be assumed to be over 21 and/or married.

The 20 schools that do inform parents of all treatment by the student health service do so for one or more of the following reasons: (a) the school believes it has a moral responsibility to inform parents; or (b) believes it has a legal responsibility to do so; or (c) believes that since the parents are paying the school bills they have a right to the information.

2. Informing the Administration: Where the student himself seeks treatment -- either general or psychiatric -- the administration and faculty of the school are generally not informed without the consent of the student unless the student is very ill, or his condition poses a danger to himself or others. Fifteen of the schools report the names of all students hospitalized in the college infirmary, but without diagnosis, medical or psychiatric. Forty-four schools report to the administration when some sort of scheduling adjustment is required, such as withdrawal from school, or a course change, or a dormitory change, but this is done with a minimum of disclosure from the student's record. The medical service might request a change in schedule because of "a stressful situation," or because roommates are not "psychologically compatible," without giving details about the actual conduct of the student.

However, when the administration refers the student to the mental health service, the majority of schools will inform the student at the outset that a report will be made to the dean. Many of the schools indicate that they discuss the evaluation with the student before giving it to the dean.

3. Informing Outside Organizations: Only eight American schools report that they will release medical information to outside organizations without student consent. All of the others state that they would reveal no information without student consent (or without parental consent if the student is under 21). However, this may include the routine or blanket consent that students give when they undertake treatment, or it may include a blanket consent signed in connection with an insurance application or a licensing or employment application.

Some schools say they require informed consent; that is, they call the student in and ask him about the specific inquiry and discuss the information they will release if he/she permits it. This protection, of course, is useful only when the student is still in the college. Many inquiries are made after the student has graduated.

Nineteen colleges state they will release information with student permission only on a "specific request," although it is not clear what the specificity refers to. One college among these explains that it will respond only to "specific questions" about the student. It reports that after instituting this requirement, the number of requests for information has dropped from several per week to three or four a year.

Thirteen American universities indicated that they refuse psychiatric information to an outside agency even with the student's consent. Six of these make an exception for a new therapist in another school who is continuing to treat the student. This is the position of the Psychiatry Division of the Berkeley Student Health Service:

> "Years of experience and discussion have led our staff to conclude that we cannot comply with such requests (for information and opinions about students who have used our services) and that communication about our work with students is justified only for the purpose of contributing to further psychotherapy elsewhere...Our attitude and policy about confidentiality are not affected by a student's having provided his release or consent to communication."

The practices of the majority of schools with respect to informing parents and administration officials conform to the general standards set by the American College Health Association. But ACHA standards are not followed by the majority as to releasing student medical records to outside organization. The ACHA would permit more disclosure to groups such as draft boards, insurance companies and prospective employers than the majority of colleges are willing to make.

The ACHA would give, with student consent, "more specific information about diagnosis, results of therapy and prognosis" than would be given to university admissions committees. And it would allow even further disclosure to the FBI, the Civil Service Commission and the armed forces. For these agencies, ACHA suggests "a general review of the case history along with guarded prognostic speculation in the course of an interview with the investigating agency...but even this should only be done if it is clear that refusing to give information will be seriously damaging to a former patient."

According to the survey, one of the factors which has caused stiffening of resistance to disclosure of student medical records to outside agencies has been the experience with the Peace Corps. "(It) comes armed with a student consent and asks for full information. Many of the schools that have developed new policies in recent years to avoid disclosure of records have done so because of the growing number of requests for information from the Peace Corps."

In 1974 Congress passed the Family Educational and Privacy Act (the so-called Buckley Amendment) which sets rules of confidentiality and rights of student access to records in schools and colleges, including medical records that are maintained by such institutions.

CONCLUSIONS

If free medical and health care could be delivered by doctors and paramedics on the proverbial desert island, freed from all the surrounding obligations of organized society, the citizen rights issues present would involve relatively manageable problems. In urban societies, however, the primary care providers we have described in Zone I are under many legal and social obligations to disclose personal medical data. These obligations are growing greater and greater as society tries to cope with problems of improving public health, occupational health and safety, research into diseases, evaluation of health care systems, and similar activities. In addition, most patients now have their doctor and hospital bills paid by someone else, requiring personal and medical data to be disclosed for service payment and care review.

In the face of these unavoidable realities, the records generated in primary care settings can no longer be treated solely in terms of what information doctor and allied health professionals need to do their job. Precisely because law and public norms require considerable disclosure of what is collected here, the recording of personal data in primary care can no longer be analyzed in isolation, and the delicate balances of the doctor-patient relationship treated by themselves. What is gathered and recorded must be seen today as the start of a complex process of outward communication, with medical data going into many areas far removed from direct patient care. It is to these additional uses that we now turn.

FOOTNOTES

1. Source Book of Health Insurance Data, 1974-75, Health Insurance Institute, New York, N.Y.

2. Osler F. Peterson, "An Analytical Study of North Carolina General Practice," Journal of Medical Education, Vol. 31, No. 12 (December, 1956).

3. Ralph Slovenko, "Psychotherapist-Patient Testimonial Privilege: A Picture of Misguided Hope," Catholic University Law Review, Vol. 23, No. 4 (Summer, 1974), pp. 651-654.

4. Source Book of Health Insurance Data, op. cit., p. 22.

5. Emanuel Hayt and Jonathan Hayt, Legal Aspects of Medical Records (Berwyn, Ill.: Physicians' Record Co., 1964).

6. James B. Lucas, "Venereal Disease Survey Contains 'Surprises'," Consultant (October, 1972).

7. Melvin H. Rudov, et al., "Medical Malpractice Insurance Claims Files Closed in 1970," in Medical Malpractice, Report of the Secretary's Commission on Medical Malpractice (Dept. of Health, Education and Welfare, 1973), Appendix Volume, p.2.

8. U.S. Bureau of the Census, Statistical Abstract of the United States: 1973 (U. S. Government Printing Office, 1973), p. 74.

9. Medical Record Departments in Hospitals (Chicago, Ill.: American Hospital Association, 1972).

10. Ibid.

11. This figure from the American Medical Record Association for 1974.

12. Lawrence Weed, Medical Records, Medical Education and Patient Care (Cleveland: Case Western Reserve Press, 1969).

13. Barry Decker and Paul Bonner, (Eds.) PSRO: Organization for Regional Peer Review (Cambridge, Mass.: Ballinger Publishing Co., 1973).

14. Joint Commission on Accreditation of Hospitals, Hospital Accreditation References (Chicago, Ill.: 1964), pp. 109-110.

15. As reported in the New York Times, November 3, 1974, p. 33.

16. J.S. Zawacki, The System of Unofficial Rules of a Bureaucracy: a Study of Hospitals, (Unpublished Ph.D. Dissertation, University of Pittsburgh, 1963) pp. 194-205.

17. Hayt and Hayt, op. cit.

18. Hospital Handbook on Birth and Fetal Death Registration, Public Health Service, Dept. of Health, Education and Welfare (Rockville, Md.: Center for Health Statistics, 1973).

19. Communication from Michael A. Baker to Project.

20. Kai T. Erikson and Daniel E. Gilbertson, "Case Records in the Mental Hospital," in Stanton Wheeler (Ed.) On Record: Files and Dossiers in American Life (New York: Russell Sage Foundation, 1969) pp. 389-414.

21. As reported in the New York Times, June 18, 1975, p.26. See also, "Nursing Homes: Haven or Hell?" State Government News, Council of State Governments, October, 1975, p. 2.

22. "A Report on Taylor House," (mimeo), American Civil Liberties Union of the National Capital Area, Washington, D.C., May, 1973.

23. Department of Health, Education and Welfare, "Rules and Regulations for Skilled Nursing Facilities," *Federal Register*, Vol. 39, No. 193, October 3, 1974.

24. See the Los Angeles County Medical Center profile, in this Report, *infra*.

25. *Medical Record Departments in Hospitals*, *op*. *cit*.

26. *Ibid*.

27. President's Commission on Law Enforcement and the Administration of Justice, *The Challenge of Crime in a Free Society* (Washington, D.C. 1967) pp.220-221.

28. U.S. Public Health Service, *Funeral Directors' Handbook on Death and Fetal Death Registration* (Rockville, Md.: National Center for Health Statistics, 1967).

29. Eleanor Ann Schuster, *Privacy and the Hospitalization Experience*, (Ph.D. Dissertation, University of California, San Francisco, 1972).

30. *Roe v. Wade*, 410 U. S. 113 (1973).

31. Telephone conversation with staff attorney, ACLU of Northern California, June 10, 1975.

32. *Hammonds v. Aetna Casualty and Surety Co*., 243 F. Supp.793 (N.D. Ohio, 1965).

33. George J. Annas, "Judicial Treatment of Medical Records and Doctor-Patient Communications," Memo to Project, 1975.

34. *Ibid*.

35. Edna K. Huffman, *Medical Record Management* (Berwyn, Ill.: Physicians' Record Company, 1972), Chapter 4.

36. *In Re Lifschutz*, 2 Cal. 3d 415, 467 P. 2d 557 (1972).

37. Annas, note 33 *supra*.

38. Annas, note 33 *supra*.

39. *Clark v. Geraci*, 208 N.Y.S. 2d 564 (S. Ct. N.Y. 1960).

40. *Hague v. Williams*, 181 A. 2d 345 (N.J., 1962).

41. Annas, note 33, *supra*.

42. *Iverson v. Frandsen*, 237 F. 2d 898 (10th Cir. 1956).

43. *Simonsen v. Swenson*, 177 S.W. 831.

44. As reported in the *New York Times*, July 31, 1974.

45. *Tarasoff v. Regents U.Cal*., as reported in 43 *U.S. Law Week* 2289 (Jan.14,1975).

46. J.R. Waltz and F.E. Inbau, *Medical Jurisprudence* (The MacMillan Co., N.Y.,1971) pp. 275-276.

47. As reported in the *New York Times*, September 30, 1973.

48. 8 Wigmore, *Evidence* Sec. 2380a.

49. Rule 501. See 43 *U.S. Law Week* 1105 (January 15, 1975).

50. *Barber v. Time, Inc*., 159 S.W. 2d 291 (Mo. 1942)

51. Bazemore v. Savannah, 155 S.E. 194 (Ga. 1930).

52. Banks v. King Features Syndicate,Inc., 30 F. Supp 353 .

53. Feeney v. Young, 181 N.Y.S. 481 (App. Di[illegible] N.Y. 1920).

54. Griffin v. Medical Society of State of New York, 11 N..Y.S.

55. Horne v. Patton, 287 So. 2d 824 (Ala. 1973) .

56. Annas, note 33, supra.

57. The background of the enactment of this law is described by Curran et al, "Protection of Privacy and Confidentiality," 182 Science 797 (1973).

58. 42 U.S. 242a.

59. People v. Newman, 32 N.Y. 2d 379, 298 N.E. 2d 651 (N.Y. Ct. App.1973).

60. Letter from Richard P. Bergen, Director, A.M.A. Legal Research Department, to Boston attorney Garrick F. Cole, June 18, 1974.

61. Letter from Dr. Simon Auster to Virginia Legislative Committee,

62. Mass. G.L., Ch. 111 Sec. 70.

63. As reported in the Boston Evening Globe, March 1, 1974, p.1.

64. "Patients' Rights: Access to Hospital Records," Report by the Massachusetts Public Interest Research Group, Aug. 12, 1975.

65. Access to Medical Records, Report of the Secretary's Commission on Medical Malpractice (U.S. Government Printing Office, 1973) p.75.

66. Pyramid Life Insurance Co. v. Masonic Hospital, 191 F. Supp. 51 (W.D. Okla.1961).

67. Matter of Weiss, 47 N.Y.S. 2d 455 (1955).

68. Emmet v. Eastern Dispensary and Casualty Hospital, 396 F. 2d 931 (U.S. App. D.C. 1967).

69. Morris v. Houster, 377 S.W. 2d 841 (Tex. Civ. App. 1964). A similar result was reached regarding the patient's right to inspect university health records at the University of Texas, Morris v. Smiley, 378 S.W. 2d 149 (Tex. Civ. App. 1964).

70. As reported in the New York Times, April 23, 1973.

71. Gotkin v. Miller, 379 F. Supp. 859 (1974).

72. Access to Medical Records, op. cit., p. 181.

73. Robert M. Veatch, "Medical Records: Patients Rights and Responsibilities," Institute of Society, Ethics and Life Sciences, Hastings, New York.

74. Letter from an attorney with the Suffolk County chapter, New York Civil Liberties Union, July 30, 1974.

75. Cited in Fleischer, "The Ownership of Hospital Records and Roentgenograms" 4 Ill. Cont. Legal Ed. 73, 82 (1966); and McGarry v. Mercier, 272 Mich. 501, 262 N.W. 296, (1935).

76. Natanson v. Kline, 186 Kan. 393, rehearing denied, 187 Kan. 186 (1960).

77. Hagman, "The Medical Patient's Right to Know," 17 U.C.L.A. L. Rev. 758, 764 (1970).

78. *Canterbury v. Spence*, 464 F 2d 772 (D.C. Cir. 1972); *Wilkenson* v. *Vesey*, 295 A. 2d 676 (R.I. 1972); and *Cobbs* v. *Grant*, 502 P. 2d 1 (Cal. 1972).

79. See generally, G. Annas, "Informed Consent: When Good Medicine May Not Be Good Law." 1 *Medicolegal News* 3(1973).

80. *Cobbs* v. *Grant*, supra.

81. *Natanson* v. *Kline*, supra.

82. *Canterbury* v. *Spence*, supra.

83. Frank A. Schneiger, "Liberal Social Change In a Conservative Bureaucratic Setting: A Case Study of the New York City Prison Health Program," Unpublished Ph.D. Dissertation, Columbia University, 1976.

84. Tom Wicker, *A Time to Die*, New York; Quadrangle Books, 1975), p. 81.

85. *The Seeds of Anguish: A Study of the D.C. Jail*, (Washington, D.C.; ACLU of the National Capital Area, 1972).

86. Schneiger, note 83 *supra*.

87. Conversation with Arpiar Saunders, November 15, 1975.

88. David B. Knoll, "The Physician-Patient Privilege, Article 31 and the Military Doctor ," *Military Medicine*, Vol. 136, (July, 1971), pp. 640-643.

89. Affidavit filed with Lawyers Military Defense Committee, June 28, 1974.

90. Aryeh Neier, *Dossier*,(New York; Stein and Day, 1975) appendix.

91. This account of IBM practices comes from internal IBM memoranda, including: "IBM Medical Department," "Managing Personal Information in IBM," and "The Privacy Training Package"; and a working paper: "A Report of Employee Privacy Within the IBM Corporation," prepared for a Symposium/Workshop sponsored by the Department of Commerce, the National Bureau of Standards and the Mitre Corporation, April 2-4, 1975. Internal documents used with permission of the IBM Corporation.

92. William J. Curran, "Policies and Practices Concerning Confidentiality in College Mental Health Services in the United States and Canada," *American Journal of Psychiatry*, (May 1969).

CHAPTER 2. ZONE II - SERVICE PAYERS AND HEALTH CARE REVIEWERS

Medical records in Zone II are not used for the delivery of primary health care by government and private agencies. They are used for two separate but closely related purposes. The first is for the payment of health care for those individuals eligible for medical benefits under government programs or private insurance plans. The second is to monitor the costs and quality of care given to these patients.

Medical Service Payers

One hundred ninety million Americans are covered by some form of public or private health insurance. The estimated total cost of this insurance is $57 billion dollars a year. Health insurance is not only a major American preoccupation, it is a major occupation as well: 150,000 Americans work for federal, state and local government health insurance plans; Blue Cross-Blue Shield has 70,000 employees; private commercial health insurance companies employ 500,000 people.[1]

Service payers, whether government agencies or private companies, need to have positive identification of the patient and to know what medical services he or she received. Without this basic information, they could not honor claims for benefits or reimburse doctors and hospitals. They frequently need more than this basic information to protect themselves against fraud by the patient or by the health care provider. Private companies also collect medical information and other personal data in advance of granting insurance coverage to make certain that the individual is a good medical and financial risk. What follows is a description of how service payers operate, what their sources of medical information are, and how they use the medical information they collect.

Private Service Payers

In 1973, 182 million Americans were covered by some form of private health insurance. Insurance companies provide 60% of this coverage today, Blue Cross-Blue Shield provide 44%, and other prepaid insurance plans provide 9%. (These figures add up to more than 100% because many individuals have coverage with more than one organization.) More than 75 million Americans have some form of disability insurance.[2]

Widespread as this health insurance coverage is, it is by no means universal. Some 20 million Americans have no coverage at all. Nor is coverage evenly distributed in the population. Some families are covered for only a small fraction of their medical bills, while others are enrolled in programs that provide a full range of medical services.[3] All of this means that for every individual covered by private insurance, decisions must be made as to his or her eligibility, what rate he or she should pay, and, once covered, whether claims for benefits should be paid.

Most health insurance coverage however, is not by individual policy. Group health insurance policies cover 83 million Americans, compared with only 48 million who have individual policies.[4] Employment by a particular firm guarantees health coverage at a rate common to all the employees without any requirement that individual workers provide medical information about themselves. The rate the group member pays depends not on his or her physical condition, but on decisions the employer makes about the whole group. This can affect hiring policies when employers try to keep insurance rates low by hiring the "right" kind of people. (This will be discussed in the Employment section in Zone III.)

The information obtained from the individual's application form is the major source used for health underwriting decisions. On it, the applicant may be asked to include recent hospitalizations, major illnesses, a medical history, the existence of "nervous" and mental disorders, etc.[5] No insurance company investigates all applications, although most of the larger health insurance firms check new applications against their previous applications and claims files.[6]

Little is known about what percentage of applications are checked further, or how the decision to check further is made. Mutual of Omaha, the largest provider of private health insurance, states that it checks only 5% of health insurance applications beyond the application form.[7] (Mutual's operations are described in detail in the Profiles section.)

Once a decision has been made to go beyond the application form, private insurers may check physicians' or hospital records. Insurance applicants sign a release form when they apply, giving the company access to medical records and other sources of information, and patients entering a hospital are required to sign a form giving the hospital authority to release their records to insurance companies and others.

When an insurance company finds something "doubtful" in the application, or the check of its own files, it may order a further investigation. The doubtful information could be about the applicant's surroundings or a dangerous occupation. Checks are also made when the application is for a large amount of income-protectio insurance. The investigation may be made by the company's own investigative department, but more likely it will be conducted by an outside firm that specializes in investigative reports, such as Hooper-Holmes, Service Review,Inc., American Service Bureau, O'Hanlon's Report, or Retail Credit Corporation.

The largest of these companies is Retail Credit, which employs 8,500 people in 1,600 branch offices in the United States, Mexico, Canada and the West Indies.[8] Its reports for health service payers include not only information about the applicant's health, but frequently comments about personal habits and morals, employment, police records check, income and indebtedness.

Processing of Health Insurance Claims

In the processing of claims, the patient's medical record is the chief source of information, often the only source. The health insurance industry routinely collects three types of information from the patient record:[9]

(1) patient identification, including name, address, name of subscriber, relationship of patient to subscriber, patient's occupation and employer, age, sex and identifying number;

(2) clinical information, including attending physician, referring physician, description of accident or illness, description of operations or medical procedures, and final diagnosis and complications;

(3) financial information, including length of stay, charge per day, and accommodations.

In the Blue Cross system, after this material has been used for reimbursing the patient or the hospital, the clinical information is usually separated from the identifying information and is used for actuarial ratings, claims and utilization review, administrative studies and research.[10]

Blue Cross has developed a three-level claims review procedure. Level One consists of screening all claims against established parameters of length of stay, ancillary charges and other standards which identify misutilization of services. Claims that are not approved at Level One are likely to involve unnecessary private room charges; diagnoses of chronic diseases without mention of current exacerbations; symptoms rather than diagnoses; unusually long or short hospital stays; unusually high or low ancillary charges for particular diagnoses; and Blue Cross contractual exclusions. Level One claims are reviewed by specially trained clerks.

Claims referred to Level Two are usually evaluated by Blue Cross staff registered nurses. Where length of stay is being reviewed, in addition to the established standards, the reviewer will consider the age of the patient, the hospital involved, secondary diagnoses or complications, days spent in intensive care, and use of ancillary services.

In addition, some conditions automatically call for review at Level Two. Among them are obesity, rehabilitation procedures, maternity, cosmetic surgery, pre-existing conditions, dental care, hospital stay for diagnostic purposes, and mental and nervous conditions. The mental and nervous category includes alcoholism, drug addiction, attempted suicide, psychoneurotic and personality disorders, epilepsy, migraine, colitis, convulsions, and other conditions. Final diagnoses that mention only the above require additional information before the claim is reviewed. A request is sent to the hospital for copies of physicians' orders, history of present illness, history of past illness, examination and test reports, progress notes, etc.

If a claim cannot be approved at Level Two, it is referred to Level Three for further review by a Blue Cross staff physician, who may make additional requests to the hospital for information, including the patient's entire medical record.

The reason for this three-level approach, beyond identifying those conditions that are not covered by the contract, is to review those diagnoses that most readily lend themselves to fraud by physicians and other health-care providers. Cut-and-dried medical procedures--setting a broken leg, for instance--present very few such opportunities. But illnesses that require long-term therapy, where the outcome cannot be predicted, are prime possibilities for drawing out the treatment and for exaggerating the amount of care given to increase the amount of reimbursement due to the health-care provider. While insurance companies feel that for this reason records in this category deserve closer scrutiny, the health-care providers feel that such records, especially psychiatric illnesses, should be protected against unnecessary examination because of the sensitive materials they contain.

According to a report by the American Medical Records Association in 1974:

> "There are two basic problems that severely affect the processing of claims in any Blue Cross plan and probably in all health insurance companies: insufficient information and incorrect information. Money and manpower could be saved if hospitals carefully controlled the submission of information to insurance companies; and if in turn these companies notified the hospital precisely why additional information is required."

Citizen Rights Issues

Access: Since 1971, Retail Credit and similar firms have come under regulation of the Federal Fair Credit Reporting Act.[11] An insurance company or employer who wishes to have an investigative report prepared on an applicant must notify the applicant of this fact, briefly describing the topics that the report will cover. If the applicant is turned down on the basis of information in the report, the company must notify the applicant of the name of the agency that produced the report. The investigating agency is then required to discuss each report with the applicant at his or her request. It must inform the individual of the contents of the report, but is not required to show it or to provide a copy of it.

Several exceptions under this law are important: Claims investigations are not covered. Medical information does not have to be discussed. In-house insurance investigative departments are not covered.

A Senate bill S.1840, introduced in 1975 to amend the Fair Credit Reporting Act, would end these exceptions.[12] It would require that consumers be given visual access to their files as well as summaries of their contents; it would specifically give consumers the right to the medical information in their files; it would disclose the sources of investigative reports, whether in-house or by a company such as Retail Credit; it would provide advance notice to consumers that a report is being made on them for employment purposes, and it would notify consumers at the time an investigative file is opened on them.

The amended act would require specific consent, rather than blanket consent, for the release of medical information, including a notice on the consent form that the material will be sought and kept by organizations like Retail Credit as well as the insurance company requesting the information. The proposed bill would also give the Federal Trade Commission the power to prohibit investigative reporting companies from setting quotas for derogatory information.

The number of complaints about lack of access to service payers' records has not been high, in part because policyholders seldom learn of inaccuracies in their records. It is also because--although they have signed broad release forms both as patients and as applicants--the policyholder is usually unaware of who precisely gets his medical information, and how much detail is in the medical records that are transmitted to service payers.

Confidentiality: The major issues in service payment concern the confidentiality of personal medical data. Most of these arise because of ambiguities in the ethical and legal rules governing disclosure of medical data to employers or government health funders.

There are many incidents in which sensitive medical conditions of individuals were disclosed to employers by health insurance firms.[13] Sometimes this was done directly, on the assumption that employers were entitled to know because they paid all or part of the premium. Sometimes disclosure took place through the way that initial claims processing was handled by the employers, as when an employee's supervisor had to sign claims submitted to the firm's insurance carrier; or when a medical claims unit in the personnel department considered it appropriate to inform management of certain medical conditions being claimed (psychiatric treatment, for example.) There are instances of private companies doing work that requires Defense Department clearances for employees passing on to the government information derived from medical claims that employees were receiving psychiatric care, on the assumption that this might affect the continuation of the employee's security clearance.

Dr. Maurice Grossman, Clinical Professor of Psychiatry at Stanford Medical School, and chairman of the American Psychiatric Association's Task Force on Confidentiality, has compiled a set of case incidents from the psychiatric area illustrating these leakages. Among them are the following three examples:[14]

1. "A patient, the wife of an employee covered by a group contract required intensive treatment because of extreme emotional decompensation...When her husband filed a claim for the cost of treatment, he was told that the employer would be informed of the claim and would be required to increase premium payments on all employees...The physician was dissuaded from following up on the case by both the husband and the wife for fear that the husband would lose his job. The patient became worse."

2. "A schizophrenic patient received electric shock treatment in a hospital and was able to return to work. The patient was not told the actual diagnosis

because she was still in a fragile state...The hospital sent a report of the hospitalization, including the diagnosis of schizophrenia and an account of a suicide attempt to the insurance company...which [in turn sent it] to the employer under a group contract coverage. Back at work, the patient found...that her fellow employees knew all about her illness. [She] became paranoid toward her physician and terminated treatment."

3. "A...psychiatric patient inquired from the insurance company whether information would reach the employer and was assured it would not. The entire therapy was damaged and the patient became worse when the employer disclosed knowledge of the treatment and other factors. The Medical Director of the National [insurance] company involved...wrote: 'We are obligated to tell the employer because he pays the premiums.'"

In the summary of the Blue Cross claims review process, it was noted that mental and nervous conditions were usually not approved at Level One, and that at the Level Two and Three stages, the company generally called for further medical information, sometimes including the patient's entire medical record. This project received half a dozen letters from doctors concerned about such demands for detailed data in insurance claims processing. One was from Dr. Wilson C. Rippy,Jr., a Tampa, Florida psychiatrist.[15]

"My practice of child psychiatry is somewhat different than other practitioners ...As a result of this, my profile as it comes out of the computer for Blue Cross of Florida is quite different from others...Despite extensive correspondence with [Blue Cross] and many invitations to visit and view the program first hand...[t]hey have continued to misunderstand and it sounds as if they suspect the situation as being somehow improper."

"In December, 1973, they requested photocopies of the complete medical records [of 24 children's cases]. I...wondered with them if they would really like to have their psychiatrists photograph their charts and send them off out of town to an insurance company. I offered to bring the charts personally and turn them over to another physician or group of physicians...and then bring the charts back with me at the end of the review."

Dr. Rippy explains that such a physician review was ultimately arranged in this particular case, but adds:

"I should point out, however, that hospital records of patients in the past have been photographed in their entirety, sometimes without my knowledge, and sent to Blue Cross. What eventually happens to these records, I have no way of knowing. In view of this, I have become increasingly apprehensive about what I dictate into the hospital chart, which of course compromises the chart and makes it difficult for committees made up of child psychiatrists to get an in-depth study of the patient...I really doubt whether agencies or institutions other than physicians need the details within the medical chart and continue to wonder why they have access to them. I find my patients are aware of this and apprehensive about telling me things...and I cannot really reassure them that the chart will not be copied or that the information somehow will not get out."

A similar letter came from Dr. C. Brandon Qualls, Associate Director of the Health Team Study Group at Stanford University Medical Center in California.[16] He wrote:

"Enclosed is a copy of a recent communication from an insurance company, in which they asked to film our medical records. One of our patients had signed a standard release of information form used by insurance companies and subsequently a representative of Micro-Reproduction Services visited our offices to microfilm all the patient's records. Needless to say, we refused such access...The representative was not easily put off and tried to pressure one of our staff for access to the patient's file. We subsequently contacted the patient and explained what had happened. The patient was quite surprised, because he had no idea he was granting complete access to his medical file as part of his application... and he was much relieved that we had not divulged any information..."

"More generally, we strenuously object to the wholesale reproduction and release of patients' files. Since we are a psychiatric clinic, this kind of request is a double affront to us, given the sensitive nature of the information imparted to us by our patients. We strongly feel that third parties should have access to the minimum amount of information necessary to complete their services, rather than to the maximum amount of information..."

Because doctors and patients have these concerns about the details of medical conditions being sent to service payers, individuals entitled to reimbursement sometimes do not file claims when socially stigmatized conditions are present. It has been reported that many women are not submitting insurance claims for abortions even though these are now legal. As one observer explained: "Social acceptance of abortion is still mixed, and even those who support the principle of the right to choose may be less supportive to immediate associates undergoing abortion. At any rate, the woman patient may not wish to put work-based relationships to this test; even employment may be perceived as being in jeopardy."[17]

A similar situation has been reported with regard to claims for psychiatric treatment. Benjamin Lipson, an insurance underwriter in Boston, whose firm specializes in placing "difficult" risks, has conducted surveys and studies of the effects that current health and life insurance practices have on individuals. In a recent speech on "Psychiatry and Underwriting," Lipson declared:

"Gun-shy is one way to describe the psychiatric patient who pays for benefits normally covered by his health insurance because he is frightened of a breach of confidentiality. A Maryland psychiatrist reported recently, for instance, that in the six years from 1968 through 1973, patients of his having Federal Employees Health Benefits Insurance with Blue Cross paid amounts ranging from $11,950 in one year to $13,500 in another year for psychiatric care that otherwise would be covered or defrayed by their insurance. In 1974, during only the first ten months, the figure for this one psychiatrist's patients came to $18,400. The doctor estimated that in the past ten years, his patients paid at least $150,000 out of their own pockets needlessly. And these are not isolated cases."

In response to the mounting concern about the confidentiality of service payers' medical records, some of them have begun to re-evaluate their procedures. The National Association of Blue Shield Plans, for instance, adopted a formal policy on "Guidelines on Preserving Confidentiality of Medical Records" in September, 1975.[19] The guidelines warn of "the potential threat of indiscriminate access to, and releasing of, sensitive patient data." Medical information should not be released without a court order and when there is a court order, Blue Shield "should release only the specific information requested." Medical information used for research or utilization reviews must not "identify the patient, subscriber or physician." The guidelines call for restricting access to "the least number of people necessary" within the Blue Shield organization, and for orientation and training programs which emphasize the sensitivity of medical records and the need to maintain their integrity. Perhaps most important:

"Plan employees should seek only those data necessary to adjudicate a claim, case or utilization patterns, and profiles. For example, if the Plan needs only a discharge summary or consultation report, it should not ask the hospital or physician for the entire record. To do so not only creates storage problems, but also places unnecessary burdens on those mechanisms which are meant to insure confidentiality."

Government Programs:

Almost all of the 21 million Americans over 65 are covered under one or both of the Medicare programs.[20] More than half of these have supplementary private insurance as well. Medicaid provides some medical expense coverage for millions of low-income patients. Each year, social security disability payments go to more than three million workers. HEW also provides funding, on a partly matching basis with the states, for a broad variety of special health services: for children, the mentally retarded and blind, the emotionally disturbed, the physically handicapped, alcoholics, and drug addicts. In addition more than 60 million full-time workers are covered under Workmen's Compensation laws.

For those over 65 who are covered by Medicare, once eligibility of age has been established, the program does not need to collect information on whether an individual is a poor health risk or a poor financial risk. The government's major concern is to make sure that the medical procedures it is paying for are in fact performed, and if performed, are necessary in terms of sound medical practice. This concern for fraud is directed not at the patient, but at the doctor or hospital being reimbursed. Misuse and fraud by doctors and health care providers running into the millions of dollars is often cited as a chief reason for the astronomical costs of government funded medical programs. Thus, government programs use the patient's medical record for utilization review and quality care assurance, which will be discussed shortly.

Medicaid and several of the special health programs listed above require the establishment of financial need by participants. A new amendment to the Social Security Act, Title XX, went into effect in October, 1975.[21] It requires the states to scrutinize closely the eligibility of participants in the Aid to Families with Dependent Children Program, and the Supplementary Security Income Program (the aged and the blind). State administrators are encouraged to cross-check these two categories against the records of individuals in other government programs such as Medicaid or state-supported correction services. Thus, for example, the administrator of a program for crippled children might check the eligibility of a particular child by checking the records of the juvenile justice system to make sure that the information on the latter record is the same as on the application for aid for the handicapped child.

The states may also check eligibility through other sources. In Connecticut, for example, the applicant's income documentation is checked with the records of the Connecticut Department of Labor, which collects a quarterly report on wages from each employer. But more than income documentation is required to participate in the medical benefits of these programs. Form W-2000 of the Connecticut Department of Social Services requests name, address, Social Security number, date of birth, ethnic, educational, religious and marital data. Applicants are not told that beyond identifying name, address and Social Security number, and income information, the other data are optional and not required by federal regulations. Nor are they told how this information will be used.

Most state and federal programs monitor medical aid to detect fraud, or as President Ford put it when Title XX was signed into law, "to get the chiselers off welfare." At least one government agency disbursing medical aid funds went far beyond this: Under the California Short-Doyle Act, county health departments disburse supplemental funds to psychiatric clinics on behalf of those patients who cannot afford private practitioners.[22] The Marin County Department of Health Services demanded that psychiatric clinics receiving these funds supply an analysis of each patient's problems, including the patient's living situation, whether he or she had difficulty in social relations, and answers to questions about therapy such as "What does patient expect to gain from therapy? What is patient willing to change? What is patient willing to undergo to bring about change?"

Although the California Short-Doyle Act required no such information, the Marin County Department of Health Services told the county psychiatric clinics that it would withhold the funds if the questionnaires were not completed and returned.

UTILIZATION REVIEWS AND QUALITY CARE ASSURANCE

Utilization review is a system by which hospitals and outside monitoring agencies attempt to determine how the hospital's facilities are being used, so that administrators may answer such questions as: are the overall facilities adequate to the patient load; are some facilities being underused while others are being overused; what is the normal length of hospital stay for a particular illness or operation and how do stays in a specific hospital compare with these norms; what is the staff-patient ratio and is it higher or lower than the norm.[23] Quality care assurance is the related examination of whether the treatment prescribed for the patient is appropriate, and whether the actual delivery of that treatment is along professionally acceptable lines.[24] Both kinds of reviews are needed by hospitals so that they can plan the most efficient use of their facilities at the lowest costs; to service payers so that they may control the costs of medical care; and to patients so that they may be assured good quality medical care under good physical conditions.

Utilization and quality care assurance reviews are conducted on several levels which sometimes overlap. Many hospitals conduct their own utilization reviews. Sometimes they review their internal operations alone, and sometimes they compare themselves to other hospitals so they can adjust their own practices against the norms.

A variety of private statistical review services are used by hospitals around the country for statistical profiles against which to compare their own performance. The largest of these, the Professional Activity Service, has each participating hospital extract 50 or 60 items of information from patient records in order to prepare its reports.[25] The Service covers roughly 30% of the largest short-term general hospitals, representing perhaps 43% of admissions and discharges in the country. The reports prepared by Professional Activity Service and the eight or ten similar systems for hospitals do not contain identified patient information but are statistical in character.

The Joint Commission on Accreditation of Hospitals reviews hospital performance to make sure that hospitals meet certain standards in physical plant and patient-staff ratios; to determine that patient records are current and comprehensible; and to see that correct procedures are followed as to drug orders, discharge summaries, etc.[26]

State and local agencies responsible for supervising hospitals monitor sanitary facilities and compliance with building, safety, and fire codes.[27] Some of them use patient records to review hospital costs, medical procedures and length of stay. The Public Health Service also examines patient records for its annual Hospital Discharge Survey.[28] Selected information is extracted from 250,000 patient files in 690 hospitals for this purpose.

Blue Cross and Blue Shield set norms on lengths of hospital stay for particular illnesses and procedures, and of the cost of physicians' services in hospitals for given procedures, based on actuarial studies abstracted from their subscribers' records.[29] Since the "Blues" can withhold reimbursement to the hospital or physician if they find that the norms are violated without good reason, this constitutes a powerful form of utilization review and quality care assurance.

Professional Standards Review Organizations

Since the mid-sixties, federal and state agencies responsible for Medicare and Medicaid programs have required hospitals to perform several kinds of review, including patient record review, to justify the type of care provided (e.g. inpatient vs. outpatient) and the length of time a patient stays in the hospital.[30] Fiscal intermediaries for Medicare and Medicaid (often Blue Cross, Blue Shield or private health insurance companies) have been conducting claims reviews in which the need for hospital care is evaluated after the fact, and a decision is made on how much of a particular claim the government will pay.

By the early 1970's, the soaring costs of Medicaid and Medicare--in some areas hundreds of millions of dollars more than was originally estimated--led Congress to create a special structure for reviewing the costs of medical care under these two programs. This was the genesis of the Professional Standards Review Organizations (PSRO), brought into being by Title XI of the Social Security Act in 1972 (Public Law 92-603).[31] The PSROs are designed to detect fraud and misuse of facilities by health care providers--physicians and hospitals--and to assure that proper standards of care are secured under public funds.

The format of the PSROs--physician-staffed and physician-directed commissions under the aegis of state Medical societies--was suggested by the American Medical Association as a counter-proposal to head off monitoring of medical care by government officials, especially non-medical personnel. Even though the medical profession controls this policing function, some physicians' groups and hospital organizations sought to enjoin the operation of the PSROs as an unnecessary government interference with the practice of medicine.[32] In November, 1975, the Supreme Court rejected this argument, and the PSROs are expected to become fully operational by 1976, as originally scheduled in the legislation.

Under the legislation, the Secretary of HEW is authorized to designate 206 PSRO districts throughout the country by January 1, 1976, and to establish "conditional contracts" with "a qualified organization"--that is, a non-profit professional association which represents a substantial proportion of the physicians in each area. These bodies are to set up the machinery for and to administer the program. If no non-profit association applies, HEW is empowered to contract with any other organization, a hospital, for example, to administer the program in a given area.

The PSROs initial function is to provide utilization review of hospital services, first by pre-certifying the particular hospitals for Medicaid and Medicare patients, and then by regular re-certification. They must also review the quality of care within the institution, making judgments as to whether particular procedures or tests or operations are warranted for the conditions specified, and determining whether the procedures warranted were in fact delivered. Ultimately, it is contemplated that PSROs will review all government-supported institutional care: mental health facilities, skilled nursing facilities and intermediate care facilities. They may some day review non-institutional care supported by the government, including outpatient clinics and medical home visits.

Exactly how the PSROs are to conduct reviews in each area is left flexible.[33] Where a hospital has evidenced its capability and desire to run its own review program, the PSRO can contract with the hospital to do so,and in this case, the PSRO will monitor the monitor. Where a hospital is not qualified or willing to do its own review, PSRO may either assemble a professional staff to perform the review, or it can delegate this duty on some other basis.

The legislation creates a Professional Standards Review Council in each state which has more than three local PSROs. (Massachusetts, for instance, has five local districts). This state Council will be composed of one representative from each local PSRO, four physicians, and four laymen selected by the HEW Secretary as public representatives. Two of the latter are to be recommended by the State governor. The State Council will review the local PSRO performance. Over the state Councils is a National Peer Standard Review Council, consisting of 11 physicians appointed by the Secretary of HEW which reports to HEW and the Congress on how the whole program is working.

While specific administrative arrangements may differ considerably from one PSRO to another, an example from a Northeastern PSRO may be generally illustrative. This organization covers 1,400 physicians and osteopaths, and 22,000 Medicaid and Medicare hospital admissions each year.

Most of the hospitals in this region will be allowed to do their own certification and length of stay reviews. Specially trained nurses extract the patient data needed for certification forms. If the admission of a particular patient is certified, a projected length of stay will be decided upon, and the patient and the physician will be told that expenses will not be paid for beyond that length of time unless the case is examined at a later time and re-certified. Copies of the certification forms go into the patient's file and to the PSRO. Difficult cases are referred to PSRO physicians for decision.

When the patient is discharged, medical record technicians may extract information for a discharge summary, a copy of which will be sent to PSRO. Working from this information, and occasionally from additional patient file information from the hospital, the PSRO will do medical evaluation studies and maintain profiles on patients, physicians and institutions.

According to the director of this PSRO, it is not yet clear exactly how the patient and physician profiles will be used, although it is assumed that physicians will be alerted if their practices depart substantially from those of other physicians in their region, as for example, how frequently they perform surgery for a given condition. One of the considerations here, according to the director, will be to "avoid stigmatizing individual physicians among their colleagues by directing most of the educational efforts at the entire staff of the hospital."

Since the PSROs are not yet fully operational, several aspects about their role are still to be developed. There are conflicting opinions about when and if the PSROs will eventually replace totally the present Medicaid and Medicare evaluation programs, some of which, as noted earlier, are now conducted by a variety of fiscal intermediaries.[34] Nor is it established exactly what kinds of materials the PSROs will collect for their reviews, what sort of patient record review will become standardized, and whether or not the PSRO will virtually compel the creation of state-wide or regional data banks.

CONCLUSIONS

This chapter has highlighted several features of record-keeping and data use in Zone II. The personal medical data used by service payers and care reviewers does not come directly from patients but from the records compiled and maintained by primary care providers. As a practical matter, general consent forms and the legal doctrine of implied consent result in the patient unknowingly surrendering control over what is furnished to Zone II organizations and how it is used.

Within the past year or two, medical spokesmen and civil liberties groups have voiced concern about the broad scope of Zone II demands for patient information. Among the questions they have raised are: Whether the amount of detail sought is necessary for the functions performed; whether the data is adequately secured against unauthorized third party access; and what the justifiction is for retaining patient data for long periods in identified form.

These concerns have begun to create a reconsideration of Zone II needs and practices among insurers and care reviewers themselves as well as medical societies and various government agencies. Among the possibilities being explored are whether removal of patient identifiers from many of the payment or review processes is desirable to minimize the dangers of improper disclosure; whether notification to patients of how insurers process their claim data should be required, with rights of access provided when the patient requests it; and whether there are ways of lessening the amount of personal data required for sensitive Zone II activities such as payment for psychiatric treatment or stigmatizing physical conditions.

It should be underscored that what is being re-examined is the procedure for protecting, and limiting the information supplied, and not the fundamental idea that there is a legitimate need in Zone II for identified patient information. It is almost universally accepted that any health care system --whether public or private or a mixture of the two--must know who the patients are in order both to pay for their care and to guarantee that this care meets professional standards at a reasonable cost.

FOOTNOTES

1. "The Condition of Health Insurance in the United States," introduced as part of the summary of the proposed budget for the "National Voluntary Medical and Hospital Services Insurance Act: H.R. 3252, by Rep. Robert J. Labomarsino (Cal.): Congressional Record, May 21, 1975.

2. Source Book of Health Insurance Data, 1974-75. Health Insurance Institute, New York, N.Y.

3. This is a gross estimate. The Census Bureau estimates that 80% of citizens under 65 are covered by private insurance (Statistical Abstract, 1973, p. 466). The 21 million persons covered under Medicare represent another 10% of the population.

4. Source Book of Health Insurance Data, op. cit.

5. See the profile on Mutual of Omaha, this Report, infra.

6. Ibid.

7. Ibid.

8. Albert A. Foer, "The Personal Information Market," reprinted in Fair Credit Reporting Act-1973 hearings before the Sub-committee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs, U.S. Senate, 93:1 (U. S. Government Printing Office, 1973).

9. This description of the processing of claims is taken from "Confidentiality and the Health Insurance Industry," by Mary Waterstraat and Cynthia Storm, a working paper submitted by the American Medical Record Association to the A.P.A. Working Conference on Confidentiality of Health Records, Key Biscayne, Florida, Nov. 6-9, 1974.

10. Ibid.

11. For a general description of the provisions of the Fair Credit Reporting Act, see Foer, op. cit.

12. "S. 1840 - Fair Credit Reporting Amendments of 1975," Congressional Record - Senate, June 2, 1975.

13. Maurice Grossman, "Insurance Reports as a Threat to Confidentiality," American Journal of Psychiatry, 728:1, July 1971, pp. 96-100.

14. From an incident list of confidentiality breaches collected by Dr. Maurice Grossman, Clinical Professor of Psychiatry, Stanford University Medical School, June 15, 1974, titled "Factors Concerning Consent Form Authorizing Release of Medical Information for Insurance Reports."

15. Letter to Project from Wilson C. Rippy, Jr., M.D., September 5, 1974.

16. Letter to Project from C. Brandon Qualls, M.D., 1974.

17. "Abortion Benefits Under Health Insurance and the Right to Privacy," proposal submitted by Charlotte Muller, Associate Director, Center for Social Research, City University of New York, to Rockefeller and Ford Foundation, 1975, pp.13-14.

18. Benjamin Lipson, "Psychiatry and Underwriting," paper distributed at Working Conference on Confidentiality of Health Records, op. cit.

19. "Guidelines on Preserving Confidentiality of Medical Records," adopted by the Board of Directors of the National Association of Blue Shield Plans, September 3, 1975.

20. Source Book of Health Insurance Data, op. cit.

21. "Title XX: A Major Threat to Privacy," Connecticut Medicine, Vol. 39, No. XII, (December, 1975).

22. Affidavits and documents submitted by Marin County clinicians to ACLU of Northern California, September, 1973.

23. Barry Decker, M.D. and Paul Bonner (Eds.) *PSRO: Organization For Regional Peer Review* (Cambridge, Mass. Ballinger Publishing Co., 1973).

24. *Ibid*.

25. "Hospital Discharge Data: Report of the Conference on Hospital Discharge Abstracts Systems," *Medical Care* (Supplement), July-August, 1970, Vol. 8, no.4.

26. "Joint Commission on Accreditation of Hospitals," *Hospital Accreditation References* (Chicago, Ill., 1964).

27. *Quality Assurance of Medical Care*, Health Services and Mental Health Administration, Department of Health Education and Welfare (Washington, D.C., 1973) pp. 179-192.

28. National Center for Health Statistics, *Development of the Design of the NCHS Hospital Discharge Survey*, (Rockville, Md., 1970).

29. Waterstraat and Storm, *op*. *cit*.

30. *Hospital Accreditation References*, *op*. *cit.*, pp. 109-110.

31. This review of PSRO's is taken from *Health and Privacy: Patient Records*, a Report of Current Practices with Recommendations for Changes by the Governor's (Massachusetts) Commission on Privacy and Personal Data, November, 1974, pp. 69-77.

32. As reported in the *New York Times*, November 18, 1975, p.1.

33. *Health and Privacy: Patient Records*, *op*. *cit*. also the northeastern example is based on a site visit by project personnel.

34. See the Mutual of Omaha profile, this report, *infra*.

CHAPTER 3. ZONE III - SECONDARY USERS OF PERSONAL MEDICAL DATA

This chapter traces how secondary users of personal medical data - organizations not directly providing health care, paying for it, or assuring its proper delivery - obtain such information for various business or governmental purposes, and how they use it once they get it. As we noted earlier, the outward flow of medical data into Zone III has enormous impact on people's lives. It affects decisions on whether they are hired or fired, whether they can secure business licenses and life insurance; whether they are permitted to drive cars, whether they are placed under police surveillance or labelled as security risks, or even whether they can get nominated for and elected to political office. Each of these decisions--and many more--involves a balancing of the individual's claim to privacy with other societal goals. The survey that follows catalogs existing practices, and also notes the continuing re-evaluation of these competing values that has taken place over the years, especially during the past decade of major changes in social and political values in the United States.

CREDENTIAL AND EVALUATIVE DECISIONS

Life Insurance

The decision-making process in life insurance underwriting resembles that in health insurance. Approximately 24% of the life insurance policies in force in 1972 were on a group basis and required no health information from the applicant.[1] Still others are called "non-medical" because no physical examination is required. Many companies write insurance for younger people for up to $30,000 without requiring either a medical examination or ordering a Retail Credit report. "Non-medical" may be a misleading term, however, since companies do assess the health information provided on the application form, and may order a check with the Medical Information Bureau, an industry-run medical information pool.

Since the Medical Information Bureau (MIB) is the chief source of the life insurance industry's health information, a brief explanation of its operation may be helpful.[2] MIB was established in 1909 by large insurance companies for the purpose of supplying medical reports about insurance applicants to its 700 member life insurance companies.

These member insurance companies are the source of the raw data from which MIB compiles its final reports. The reports to MIB draw on the life insurance companies' sources of information, such as applications, physicians' and hospital records, and previous claims. When an "insurance related" medical condition is noted, it is passed on to MIB through a system of more than 300 separate codes which can produce a general picture of the applicant. Family history codes permit the listing of hereditary diseases, TB, and mental disorders in the applicant's family. Blindness and other permanent disabilities are covered by other codes, as are all major infectious diseases, alcoholism, drug dependency and injuries. Until recently, codes for "reckless driving," sexual deviance and social maladjustments were included, as well as codes about financial condition and participation in hazardous sports. MIB no longer requires member firms to report information under these codes. MIB officials state that "all reports to the MIB are automatically expunged seven years after the date they are reported. In this way, reports made in the distant past are no longer available for underwriting purposes, and a mechanism is provided for a person to start afresh with a clean slate."

A typical Medical Information Bureau report might look like this: "11AG39 IND; Dr; A 14AP72; 258ZMC-340." From these codes, the insurer can tell that this individual, a physician living in Indiana, was born on August 11, 1939, and that a report was received from a medical source on April 14, 1972 that he had a psychoneurotic disorder, with two or more episodes of this problem within the last five years. The report also shows that his cardiogram is normal. Had it not been normal, specific values would have been reported. If there had been psychosomatic complications accompanying the psychiatric problem, these would have been noted.

MIB maintains files on 11 million individuals. In 1971, the Bureau handled 19 million requests for information, returning over 500,000 reports with adverse medical or other information (a little over 5%). Member insurance companies paid $9 million for these reports in 1971, and sent 2.2 million coded reports to MIB describing the health problems of applicants, or in the case of some health insurance firms, claimants, too.

In 1974, MIB adopted new rules to bring it into conformity with the Fair Credit Reporting Act.[3] The insurance applicant is now told by the insurance company that some of the information gathered about him may be submitted to the MIB. Member life insurance companies are also required to obtain authorization from the applicant before the company is permitted to query the MIB computer. Applicants are told that they may have access to the information about them, and that any inaccuracies can be corrected. When a request for access is received, MIB arranges for the company that made the report to send the information to the applicant or policyholder. Medical information is not sent directly to the applicant, but to his physician.

For deciding about larger policies or applications from older people, the full range of information sources may be used. In 1972, almost 8 million investigative reports were completed for life underwriting by Retail Credit, Hooper-Holmes and the American Service Bureau.[4] One review of life underwriting procedures indicates that firms do not check hospital records very often, even when they have a release from the patient, because it is expensive to do so.

In 1972, almost 85% of life insurance applications were approved at standard rates.[5] Of the 500,000 applications denied that year, 90% were turned down for health reasons. Roughly 4% were approved but the policyholder had to pay higher rates for the following reasons: heart disease, 35%; weight problems, 17%; other medical reasons, 29%; occupation, 9%; other reasons, 10%.

It is worth noting that very little use is made within insurance companies themselves of the information gathered during the underwriting process. Lawrence Ross suggests that relatively little information moves from one line, say life insurance, to another, say health insurance, within the same firm.[6] But both medical hearsay and reliable medical reports are used outside the insuring firm once the underwriting process is completed. Life insurance companies pass on to the Medical Information Bureau, in the form of general codes, adverse information about applicants received from Retail Credit, other companies, physician statements and medical examinations.

Automobile Insurance

One feature of auto insurance is distinctive: all states require individuals who own cars to carry liability insurance. Mandatory insurance requirements have resulted in a complex system of "assigned risks" under which everyone is supposed to be guaranteed at least the minimum level of personal liability coverage, but at higher rates.[7] A study conducted in 1974 by the Federal Insurance Administration of the Department of Housing and Urban Development showed that in spite of the mandatory insurance requirement, at the latest count (1967), 20% of the nation's drivers were still not covered by any insurance.[8] Furthermore, of the four million drivers in "assigned risk" state pools, who pay almost twice as much for automobile liability insurance, 3.3 million were "clean" risks--that is, they had not had an accident within three years. Of these, 2.7 million had neither had an accident nor a driving violation on their records within three years. The study gives no reasons why apparently low-risk individuals are refused conventional insurance, but George K. Bernstein, Federal Insurance Administrator, offered some possible explanations:

> "Applicants might be refused because a company does not want to write any more insurance in a certain area. Perhaps the company does not want to give an agency any more business. Maybe the applicant has been reported to keep a messy house. Or perhaps an individual lives in the wrong neighborhood." 9

While relatively little has been written about automobile insurance underwriting, it appears that health information plays some role in determining what rate an individual pays. Whether an individual is placed in an assigned risk pool, for example, may depend on a disability which might impair driving, or on an investigative report alleging the excessive use of alcohol. The Federal Insurance Administration report notes one insurance plan in which a family's premium would increase by 30% if the father "suffered from moderately high blood pressure."

Other factors, however, are more important than health records, according to the FIA's report: age, geographical location, race, claims history and driving violations are probably the most important reasons for forcing applicants into the assigned risk category. The American Insurance Association reported that less than ½ of 1% of its members' cancellations or non-renewals in 1968 were for health reasons.[10]

A dramatic example of a breach of confidentiality of medical records in an accident/casualty setting was revealed early in 1976. In Denver, Colorado indictments were brought against Factual Services Bureau (a 27-year old private detective agency with operations throughout the country), several of its employees, and one hospital employee for illegally obtaining information from hospital medical records.

The information was allegedly secured for casualty insurance companies and their attorneys for use in challenging claims against the companies. The most common means of obtaining the information was for a Factual Services Bureau employee to telephone a hospital pretending to be a physician from another hospital who needed the data to treat the patient whose records were on file. (One of the charges was criminal impersonation.) An Assistant District Attorney working on the case noted that it was easy to obtain hospital information without authorization because security procedures are geared to the assumption that all inquiries are legitimate, and any person calling is who he claims to be.

As of March 1976 the term of the grand jury that brought the indictments was extended for two more months and the investigation was continuing. In addition, investigations were begun in other states with the thought that this may have been a normal operational procedure for all of the company's branches.[*]

---

[*] Rocky Mountain News, January 14, 1976, p. 41, and telephone conversations with Denver Assistant District Attorney Peter Bornstein, January 22 and March 3, 1976.

Employment

To some extent, the role of health information in employment decisions follows the law of supply and demand in the labor market. The more plentiful the labor supply, the more rigid the health criteria--along with other criteria--become. Similarly, the health standards that are sometimes set by employers are often not related to their goals of reducing absenteeism, increasing worker performance, and keeping group health insurance premiums low. They sometimes appear to be an exercise in selectivity for the sake of selectivity itself.

For example, a Veterans Administration poll of company doctors recently discovered that not only medical problems like TB, diabetes and mental disorders disqualify many job applicants, but "even patients with mild illnesses, which may not increase their morbidity or mortality, are being denied work.[11] The criteria used for determining employability appear in some cases to have little relation to modern medical judgment."

Discrimination against those who have had psychiatric care has been a particular focus of protest. The American Psychiatric Association's Task Force on Confidentiality reports receiving many complaints about patients being denied employment or promotion unfairly because they have had psychiatric treatment.[12] One school system, they report, routinely denies employment to individuals who have any history of therapy or psychiatric care. The VA study mentioned above found that 75% of the 50 company physicians responding said their firms would not hire a person who "is currently under psychotherapy" for any position;[13] almost 40% reported that they would deny employment to an applicant who had previously been hospitalized for a mental illness, but was not psychotic. In a recent case in New Jersey, an applicant for the police department was rejected because his military record showed an old psychological treatment entry.[14] The impact on the job market of such restrictive employment policies can be gauged when it is recalled that almost 3 million people are currently in psychotherapy, according to a 1975 report issued by the National Institutes for Mental Health.[15]

The extent to which health information is sought by employers--often at considerable expense--demonstrates how important a part it plays in employment decisions. Health information may enter that decision-making process from at least six different sources: on the application form, from company and private physicians, from investigative reports by firms such as Retail Credit and government security agencies, from insurance claims or from the insurance carrier, from contacts with previous employers, and from U.S. military separation papers.

Many application forms demand information about the general state of the applicant's health and whether or not the applicant has ever suffered from a mental disorder, received psychiatric treatment, drinks, or uses drugs. Sample surveys conducted in 1964 and 1965 by the National Industrial Conference Board, a management society, show that more than 70% of the manufacturing and non-manufacturing firms studied require a pre-employment physical for at least some applicants.[16]

The federal government investigates many applicants through the National Agency Checks and Investigations program of the FBI and the use of "full field" investigations.[17] The full field investigation has as one of its goals the assessment of "mental stability," and investigators often interview school and private psychiatrists. While full investigations are normally conducted only for higher government posts, or in situations where there are "national security" concerns, some government agencies order them whenever they get information that the applicant has had psychotherapy or may be a homosexual, even though he or she may be applying for a relatively insignificant job. There also have been charges that if an applicant has had psychotherapy, or is a homosexual, the job for which he or she is applying may suddenly be reclassified as requiring a security clearance, as a device for disqualifying the applicant for it.

In a report in the American Journal of Psychiatry, three psychiatrists describe the procedures followed when the government orders psychiatric evaluation of an applicant for security clearance.[18]

> "Applicants are not routinely examined by a psychiatrist. The most common reasons [for requiring the examiniation] are that he was once a patient in a mental hospital, was discharged from the armed forces because of a psychiatric condition, or had been under official surveillance because of some abnormality of behavior...
>
> The relationship of the applicant and the psychiatrist is not that of patient and physician and no traditional confidentiality of communications arises. The psychiatrist should tell the applicant that their relationship is not confidential and that all information... may be revealed to the government... [T]he interview and examination are voluntary. However, a refusal to furnish relevant data may prevent any kind of a final judgment on the individual, in which event, processing of the application for clearance would be discontinued."

A somewhat different set of circumstances arose in an actual case in which an applicant for security clearance answered "no" to the question on the application form: "Have you ever suffered from mental illness?"[19] It was subsequently revealed that some years earlier he had seen a psychiatrist for a brief period. The government claimed he had lied on the form and attempted to fire him. The applicant claimed that visiting a psychiatrist was not evidence of mental illness, and that his answer had been truthful. The government then required him to have a psychiatric examination, to which he agreed, and in addition to sign a release which would give the government access to the private notes of the psychiatrist who had treated him earlier. When he balked at this, he was fired. Ultimately the U.S. Court of Appeals upheld the government's right to fire him, but remarked that the government's practice of requiring access to his private psychiatrist's notes was not a good one, and suggested that the government re-think its procedures.

As noted earlier, for many years the U.S. military services included code numbers on veterans' discharge papers that labelled them with any one or more of a number of derogatory "medical" terms.[20] While the Services have promised to stop doing this, veterans must affirmatively request to have their discharge papers changed to omit these code numbers. Since the majority of veterans probably still do not know the meaning of the numbers, hundreds of thousands of them are carrying around this adverse information and disseminating it to employers' files.

The insurance claims process also gives employers health information on their employees. This happens either because insurance companies supply it directly to the employer as the payer of the health insurance premium, or when the personnel department of the company actively monitors claims.

In 1970, the Retail Credit Company completed more than one million reports on job applicants and candidates for promotion; for these, investigators gather health information from former employers, neighbors, personal references and workmen's compensation files.

In hearings before a House Committee in 1968, Retail Credit supplied a fictitious model report. This noted that the applicant had a period of unemployment caused by a "mild nervous breakdown" for which his physician had recommended a period of complete rest. Under the heading of "Health Habits" the report reads:

> "Mr. Bowers has good general health with the exception of a nervous disorder that has shown up previously when he has been under pressure. This usually results in stomach discomfort. His physician has diagnosed this as 'nervous tension'. He has had this condition for the past 15 years known. Subject has not suffered a relapse of nervous breakdown, however, he will take medication prescribed for relief of tension when he feels it necessary.
>
> Mr. Bowers is a social drinker, taking a maximum of 2-3 mixed drinks during any one occasion at parties and when friends visit at his home. He has never drunk to any degree of excess and does not use drugs other than medication prescribed for relief of nervous tension." 22

The report notes that the health information was obtained from his present and a former employer and "personal associates."

Not all Retail Credit reports are as detailed as this specimen. Some may use single phrases: "spleen problems," "wife has colitis, nerves," "eye injury," to describe health problems learned about from the applicant or from an employer or neighbor.

About 80% of the information in Retail Credit reports comes from the 45 million records stored in branch offices. Where the requested name is not on file, or the material needs to be updated, investigators interview the applicant and his neighbors and employers.

In 1974, the Federal Trade Commission filed a complaint against Retail Credit sharply criticizing some of its investigative and reporting techniques. Among other things, the FTC charged that:

1. Retail Credit investigators give individuals the impression that they are being investigated only in connection with a specific job application or insurance application when, in fact, the information about the individual will be kept on file by Retail Credit for future reference by any subsequent customers. Specifically as to medical information, patients are given the impression that when they sign authorizations for release of medical information, such information is for the exclusive use of the insurance company. Doctors and hospitals are also given the impression that Retail Credit is collecting information for that exclusive use. The FTC complaint states that "some consumers would not have authorized the release of such confidential information had they known it would be...utilized by...a consumer reporting agency."

2. Retail Credit gives customers (insurance companies, employers, etc.) the impression that its investigators have personally interviewed all of the individuals listed as "sources" on their reports, and have personally observed the home and environment of the individual being investigated. In fact, the FTC alleged, much of the information is gathered over the telephone, and sometimes not even telephone interviews are conducted with the listed sources. Often site visits are not made, even though the report described the house and neighborhood. If customers realized how superficial and/or inaccurate these reports are, the FTC claims, they would not rely on them to deny employment or other benefits.

3. According to the FTC, certain procedures in the preparation of Retail Credit's investigative reports encourage inaccuracy, including:

o setting quotas for the percentage of consumer reports that must contain derogatory information;

o requiring investigative personnel to complete an unreasonably high number of investigative consumer reports in a limited time;

4. Retail Credit makes it difficult for consumers to review the contents of their records by refusing to make them available at regular offices, and referring inquiries to "branch" offices which are usually very far away from where the consumer is located. The FTC states that even when such disclosures are made to consumers, re-investigations are not made, and inaccuracies are not corrected.

The FTC complaint is still being heard but W. Lee Burge, Chief Executive Officer of Retail Credit (now renamed Equifax) responded publicly to the FTC charges in his testimony at the Senate hearings to consider amendments to the Fair Credit Reporting Act.[24] Mr. Burge defended the investigative techniques of his company and specifically denied that it sets quotas for derogatory information. In his comments on the proposed amendments, he stated that the present law serves consumer needs for access adequately, and that changes would injure the consumer. The proposal for advance notification of an employment or insurance investigation, for example, would delay, for both the customer-company and the consumer, decisions on employment to the detriment of the job applicant, and might result, Mr. Burge said, in a motorist driving an uninsured car.

As to the requirement for disclosure of sources of information, Mr. Burge responded that if Retail Credit could not promise confidentiality to its sources, they would inevitably dry up. He gave as an example the consumer who is engaged in underworld activity who, if told the source of an unfavorable comment, might intimidate or physically harm the informant. Mr. Burge added that such a requirement of disclosure would also shut off sources of favorable comments as well as unfavorable ones.

Maintaining Medical Records in Health-Hazardous Industries

Medical record-keeping in employment can be of vital importance not only from the point of view of individuals securing jobs,but for maintaining good health on the job.[25] In the last twenty years, scientists have been uncovering compelling evidence that exposure on the job to certain widely used industrial products--asbestos and vinyl chloride among them--causes an alarmingly high incidence of cancer. One of the chief problems in controlling the disease is that it usually does not surface until twenty or more years after exposure. That makes careful medical record-keeping essential. Initially, the goal of the managers of the industries that use these products was to play down their connection with cancer, and to this end, many companies kept no health records at all. Dr. Irving Selikoff, one of the leading researchers in this field, tried to secure medical and employment records of workers in an asbestos plant after 17 of his private patients died of cancer after having worked there. He wanted to track down the other 700 workers so that they could be x-rayed for the disease. The president of the asbestos company told him that no such records were available.

Increasing pressure from the medical profession, especially from articles in scholarly journals, and from the Occupational Safety and Health Administration of the Labor Department and the AFL-CIO Industrial Union Department, forced the asbestos industry to permit x-raying of workers in many plants. But the workers were not told why they were being x-rayed, nor were they told what the safe levels of asbestos dust were, nor that the government had required those with the greatest exposure to wear respirators. Physicians and other health professionals were hired to examine workers, but their findings were not shared with the individual workers examined, nor were atmospheric tests shared with their medical colleagues.

The secrecy of medical findings, including the lack of access to the workers to whom the information is a life-or-death matter, brought a stinging rebuke from Jacob Clayman, secretary of the AFL-CIO Industrial Union Department, in a speech on the relationship of vinyl chloride to cancer:

> "Multi-corporate studies of cancer from vinyl chloride were initiated secretly in this country and in Europe... Their results could probably still be a secret without the presence of the mass media and if the law did not require the reporting of occupational disease [the Occupational Health and Safety Act]..."

Most often, when charges are made that medical care and medical record-keeping in employment are serving the interests of employers, and not of the employee/patient, the complaint is about lack of confidentiality of patient records. In the industrial chemical field, the charge is the same, but the complaint is lack of access.

Licensing

All states have some licensed occupations for which the health of applicants is deemed relevant.[26] Where employees deal with the public, it is generally required that they be free of communicable diseases. Thus, in many states, barbers, nurses, hospital workers, food handlers and others have to be tested for such things as TB and VD. In some states, dental hygienists are tested for these diseases when they initially apply for a license.

Psychological criteria also play a role in licensing decisions. Taxi drivers in New York City are checked through state fingerprint files to see if they have ever been a patient in a state or county mental institution.[27] Such a check is possible because identifying information on all patients admitted to government psychiatric facilities is routinely forwarded to state law enforcement files. Identification records from mental hospitalization files in Michigan are similarly available.[28] In a recent case, a court decided that an ex-mental patient could not be refused a hack license by the New York City Police Department solely on the ground of his prior "mental illness."[29] Even so, the ex-patient got his license only by agreeing to submit to a psychiatric examination every six months.

The role that medical information can play in driver licensing is illustrated by the recent controversy surrounding the adoption of new motor vehicle regulations in Maryland.[30] The original draft of the regulations required those applying for or renewing a driver's license to list past treatment for the following conditions: cerebral palsy, diabetes, epilepsy, multiple sclerosis, muscular dystrophy, heart condition, stroke, disabling arthritis or rheumatism, drug or narcotic addiction, mental or emotional condition, mental retardation, multiple sclerosis, and alcoholism. In addition, the Motor Vehicle Administration implemented the information gathering by supplying Maryland doctors with reporting forms to be sent to the Motor Vehicle Medical Advisory Board when they encountered patients with disorders characterized by lapses of consciousness. The Medical Advisory Board also received complaints filed by judges, law enforcement officers and citizens, the most frequent reports coming from family members concerned that poor eyesight of elderly people and alcoholism made their relatives unsafe drivers.

As a result of protests from psychiatrists and other members of the medical profession, arthritis, rheumatism, mental or emotional condition, and mental retardation were removed from the list of reportable conditions in the regulations finally adopted. For those remaining conditions, the license applicant must secure a physician's certificate describing the diagnosis and prognosis of the disease, along with the medication prescribed. If the license is refused or revoked on the basis of the certificate, the applicant is entitled to a hearing before the Medical Advisory Board to introduce medical evidence to support the granting of the license. In response to an inquiry from the Maryland ACLU, William T. Bricker, Deputy Administrator of the Maryland Department of Transportation stated that "while all records of the Motor Vehicle Administration are public records...the sole exception are Medical Advisory Board records."

Most state motor vehicle departments report license suspensions and revocations to the National Driver Registration Service of the Department of Transportation. These reports include instances in which licenses are revoked because of mental and physicial disabilities.[31]

THE JUDICIAL PROCESS

We have already discussed the doctrine of privilege, describing its relative standing in the common law, and the statutory exceptions that permit physicians to testify on many matters from the patient's record. All state privilege statutes contain exceptions that cover criminal proceedings so that medical testimony and medical information can be introduced.[32] In most such cases, a non-medical issue is at stake: to connect an individual with a crime, for instance, the prosecution may introduce the defendant's previous history of narcotics addiction. Defense lawyers may enter an insanity plea, necessitating psychiatric testimony or the introduction of psychiatric records. Either defense or prosecution may attempt to impeach a witness by introducing evidence about his or her psychological condition.

In civil suits, the medical condition of the individual is often the principal focus of the proceedings.[33] When someone makes his own physical condition an issue in a law suit (e.g. by bringing a personal injury or malpractice action) most courts will permit examination of the plaintiff's physician. Medical records may also be subpoenaed in such suits.

In civil commitment proceedings, of which there are thousands every year, some kind of examination report from a court-appointed psychiatrist may supplement a complaint from police or family members.[34] In their examinations, court psychiatrists sometimes draw on hospital reports. Sometimes complaints are made that such commitment proceedings are all too often purely pro forma; it is alleged that some psychiatrists do not in fact conduct independent examinations of the patient, but merely "rubber stamp" the complaint from the police or the family or other laymen. This creates a court record that the individual committed is a danger to himself or herself or to others, which becomes a part of the medical record. Thus the individual is permanently marked by a decision which appears to be a medical one, but which may in fact not be.

Medical record information is also introduced into quasi-judicial proceedings such as disability hearings, probation hearings, and workmen's compensation reviews.[35] The medical files assembled for permanent disability cases are often particularly extensive, with reports from personal physicians supplemented by those from government-appointed physicians and military records.

What are the substantive issues raised by the increasingly widespread use of medical record information in the courts?

(a) The doctor-patient relationship. Physicians, and especially psychotherapists, argue that the therapeutic process depends upon trust and that this trust is undermined by fears that therapists may testify about patients in court. When the new rules of evidence were proposed for federal courts, psychiatrists were able to convince its framers in Congress that even if communications between medical doctors and their patients were not to be privileged, it would still be necessary to privilege psychiatric communications.[36]

(b) Irrelevant and extraneous medical records. Psychiatrists and medical doctors are resentful about producing confidential medical records in court for what seem to them frivolous reasons. For example, in some divorce proceedings, a pro forma complaint of "mental cruelty" is lodged.[37] Attorneys sometimes use this as an excuse to subpoena medical or psychiatric records which are irrelevant to the real issues of a divorce proceeding. It must be noted, however, that mental cruelty is not always a legal fiction invoked to satisfy a particular state's divorce laws. Mental cruelty can in fact be inflicted by one family member on another and may play a crucial role in custody cases.

Patients and medical professionals also complain about the lack of specificity in subpoenas for medical records, and the fact that entire medical records are photocopied for the court, rather than those portions that are relevant. The responsibility for such irrelevant materials reaching court, some commentators say, lies as much with physicians and hospitals as with lawyers.[38] They note that health professionals respond too readily to subpoenas. Instead of requiring each to be justified in court and challenging those which are not specific enough, they are likely to turn the whole record over without protest when confronted by a subpoena.

(c) Informed Consent. As previously noted in our discussion of privilege, a California psychiatrist, Dr. Joseph Lifschutz, was sentenced for contempt of court after his refusal to testify about a previous patient.[39] Lifschutz argued that genuine informed consent to the release of information from therapy records was not possible and that the therapist should be allowed to refuse testimony when he or she felt it in the best interests of the patient. A more recent challenge to that ruling, now in the appeals courts, involves a psychiatrist who refused to answer some of the questions put to him about his patient.[40] His appeals brief argues that informed consent is not possible because the patient "...has no knowledge of what Dr. Caesar's answers to questions about her might be. Many patients in psychotherapy...may tell their therapist things they perceive unconsciously which are in fact not true...or they may have no recollection or a very erroneous recollection of what they have told their therapist."

(d) Physicians' Privacy. As noted earlier, confidentiality of patient records is seldom at stake in malpractice suits, since the patient is eager to waive it. What is at stake for the medical community is the physician's claim to privacy. Of special concern to them is that tissue-committee reports and other internal review committees which evaluate physicians' performance with respect to whether the appropriate diagnosis was made, etc., will be used against them in court proceedings.[41] Opponents of courtroom availability of such documents argue that it would undermine the voluntary cooperation of physicians with essential evaluation committees, and that the evaluations themselves are subject to misinterpretation. Proponents claim that the patient has the right to know if his physician has been criticized by his peers for incompetence or negligence.

PUBLIC HEALTH REPORTING

We have already mentioned how public health reporting requirements affect medical record-keeping,and discussed the subject in the context of its being an exception to the confidentiality doctrine. Nothing more needs to be added about this subject here except to emphasize that the areas where public reporting is required by law have been growing steadily during the past decades and are likely to continue to increase.

THE MEDIA

We have also discussed the use of medical record information by the media in the context of the "public right to know" exception to confidentiality. The American Hospital Association has published guidelines for the release of patient information to the media which suggest the following procedures:[42]

- A prohibition on the inspection of hospital records by media representatives.

o A prohibition on interviews or photographs of the patient without the signed consent of the patient and his immediate family. Even when patient or family consent is given, the hospital should overrule them if it feels the patient's condition may be jeopardized.

o No release of information to the media by Emergency Room personnel.

o Information released in hospital bulletins should be limited to name, address, occupation, sex, age, and marital status; and a one-word description of the patient's condition as "good," "fair," "serious," or "critical". The nature of the injury may be given but not the details (e.g. head injury, but not whether the skull is fractured; poisoning, but no statement as to the circumstances or kind or about motives.) The guidelines would prohibit any mention of a patient's having been intoxicated, or whether there was a suicide or attempted suicide.

o Hospitals should refer media requests for information in accidents and criminal cases to the police, or in the case of death, to the coroner's office, but only after notification of the immediate family.

The AHA's guidelines on prominent patients state:

> "A person whose activity is a matter of public interest, or whose livelihood or success depends on his being kept in the public eye, forfeits...to an undefinable degree...rights of privacy generally ascribed to a less prominent person."

While the guidelines suggest that patient permission is still necessary before the hospital can release information about prominent people, they go on to say that "the hospital has the added obligation of pointing out to the patient that his hospitalization is likely to become known and...public acknowledgment will usually be in his best interests... [to assure] that accurate information [about] his condition will come from an authorized source."

Reporters usually are not given access to hospital records and they usually do not depend solely on hospital bulletins for their medical information. The variety of other sources from which reporters get their information is a commentary on the looseness with which confidentiality is all too often guarded. Reporters say they get medical record information from police officers, from tipsters on hospital staffs, from military records, and from the Veterans Administration.[43] In one case, the Veterans Administration opened the medical record of a hold-up suspect to the press, with the result that his treatment for psychiatric troubles and venereal disease was publicized in the New York Times.[44]

Another factor is that there is a double standard about information released to the media. Criminal suspects, state mental patients, prisoners, and welfare clients have all made complaints about the release of their medical records. ACLU Director Aryeh Neier writes of a recent case in which a detailed description of a murder suspect's psychological problems was provided to the press by his prison psychiatrist.[45] It is not surprising that people in custody, where the health provider's loyalty is engaged by the institution instead of the patient, should be disfavored when it comes to release of confidential medical information.

LAW ENFORCEMENT

Patients' medical records are a natural resource and temptation to law enforcement officers. They provide a logical place, for example, to start looking for missing persons; to get information from victims of a crime; to identify drug abusers and through them to locate drug distributors; to track down illegal aliens; or to identify suspects thought to have psychiatric problems.

In some states, the law specifically provides that police may get certain kinds of information from medical files. The California Business and Professional Code, for instance, requires physicians to keep a record of the disposition of dangerous drugs for three years, and to keep the records open to law enforcement officers.[46] In other cases, the law allows access to medical files when the court decides that this is necessary.[47] In many states, the law is not clear, and this allows law enforcement officers to make use of medical files, at least for identification and location of a suspect, with relatively little resistance. In the Los Angeles Medical Center, as described in the Profile section, there is a police officer stationed full time in the medical records room of the hospital for the sole purpose of checking medical records for law enforcement purposes.[48]

A recent study of three large Philadelphia hospitals by R.J. Nathan illustrates that there is sometimes a large gap between official hospital policy and everyday practice when it comes to making medical records available to law enforcement officers.[49] For example, the official policy at Pennsylvania Hospital, as stated by its Medical Record Librarian, is:

> "Medical records are the property of the Hospital. The information recorded in the patient's medical records is of a highly confidential nature. Such information should not be disclosed to anyone without the written consent of the patient. Even with the patient's consent, information of a personal or privileged character should be given only after careful consideration of its value in determining the issue in question."

Included in that policy is a guideline that confidential information will not be released to the Philadelphia Police Department. But in practice, each hospital admitted its cooperation with the District Attorney's office "if there is an investigation going on." What constitutes an "investigation" is apparently the mere act of phoning the Medical Records room and requesting information. The police are well aware of this procedure and hardly ever make the initial request; rather the D.A.'s office will make the call.

Several years ago, following a disturbance at the Board of Education, some of the participants in the demonstration--black high school students--were injured by the police and either taken to Pennsylvania Hospital or got there on their own. After they were treated and released, a police captain called and asked the names and nature of the treatment. The Record Administrator refused to supply the information, admonishing the captain that "he should know better." Three days later, a member of the District Attorney's staff called and the information was readily provided with no further "inconvenience."

Mr. Nathan's study further notes that although the Selective Service System is specifically excluded from access to patient records in all three hospitals, discretionary administrative decision-making "will inevitably divulge confidential material to either local or state [Selective Service] systems and to federal agents of the U.S. Attorney's office conducting [draft-evasion] investigations."

Hospitals are not the only places where law enforcement officers are given access to medical records. Many high schools, especially inner city schools, have one or more police officers permanently stationed in them and they are given access to student files, including medical records.[50] Law enforcement officers also seek information from insurance companies' records--usually location information--although they sometimes ask and receive information about the nature of an individual's health problems.[51]

Drug rehabilitation clinics are also likely targets for police investigation, as the case of People vs. Newman, already described, illustrates.[52] The FBI recently circulated a leaflet to physicians containing detailed medical information about members of the Symbionese Liberation Army with the statement: "If any of the above individuals consults you for medical treatment, you are requested to notify your local FBI office."[53]

In 1972, the FBI placed advertisements in two AMA journals describing a woman wanted for conspiracy who had a particular skin condition for which she might seek treatment.[54] Physicians were asked to contact the Bureau if they identified her among their patients. Protests against the ads not only challenged this specific instance of cooperation, but raised the question of what might happen to the doctor-patient relationship in the medical profession if it were believed that such cooperation was routine.

Our society accepts a certain amount of law enforcement access to confidential medical records. The public reporting requirements bear this out. What is not clearly defined is at what point and under what circumstances this access becomes an intolerable intrusion on citizens' rights. If the decision is for more tightly controlled records, then it seems clear that the only way to secure it is by specific legislation such as the Comprehensive Drug Abuse Prevention Act, which was invoked in the methadone clinic case, or the statute drafted in New York to protect psychiatric records in the Multi-State Information System (MSIS).

MEDICAL RESEARCH

Americans are generally sympathetic to serious research and to medical research in particular. Between 1950 and 1970, public and private expenditures for medical research increased nearly twenty-fold, from around $100 million to nearly two billion dollars a year.[55]

A great deal of medical research requires identified records on research subjects, either because the medical treatment of specific individuals is being followed in a clinical setting, or because samples of research respondents are drawn from lists of patients or clients, or because specific individuals are being followed over long periods of time.[56]

The story of one medical research project conducted by staff members of a Chicago hospital between 1950 and 1952 illustrates how crucial identified patient records can be.[57] During those two years, 840 women were given a female hormone called stilbestrol as part of a clinical experiment to discover whether the hormone was helpful in preventing the complications of pregnancy. The women were not told that they were part of an experiment and none were aware that they were its subjects. In 1971, scientists discovered "a highly significant association between treatment of the mothers with stilbestrol and the development of vaginal cancer in their daughters." Because identified patient records were kept on this experiment, the hospital was able to track down the patients (although they would not release figures about how many they could not trace) so that their daughters could have frequent checkups to detect any early cancer symptoms.

This experiment also highlights the various civil liberties issues involved in medical research: the problem of informed consent, for example, when a group of terminally ill patients were injected with live cancer cells without informed consent;[58] the problem of truly voluntary consent, which is raised whenever prison inmates are "encouraged" to "volunteer" to participate in the testing of new drugs;[59] the question of the propriety of withholding treatment from patients for research purposes, tragically illustrated by an experiment in which a group of men was allowed to go for many years without treatment for syphilis so that researchers could study the course of the disease.[60]

Some other complaints have surfaced over extracting data from records for research purposes without securing advance, informed consent. In one case, a law professor received permission from a judge to examine court files of 189 randomly selected cases concerning mental illness commitments, including the psychiatric reports that were part of the proceedings.[61] When the research was challenged in court, the majority held that (1) those who had submitted information to the court file had no way of knowing that it might be used for purposes beyond the commitment proceedings; and (2) that notice of the proposed research would have to be given to all parties concerned if there was a reasonable possibility that the patients, families, or physicians involved would object to the researcher's access.

Concerns about uses of patient files outside the hospital are also reflected in the guidelines of a number of professional associations such as the American Hospital Association, the American Medical Association and the American Psychiatric Association, as well as in the rules of research sponsors such as the National Science Foundation and the National Institutes of Health.[62] Generally, however, the number of publicized cases of harm from the release of medical data for research is so small that few challenges are mounted to such disclosure. In some recent model legislation to protect psychotherapeutic communications, lawyers for the Mental Health Law Project stated that as long as hospital administrators reviewed the intent and procedures of research projects, the use of identified patient records in such projects was legitimate.[63] "A requirement that researchers obtain authorization from each patient would unduly burden research efforts," they said.

However, some psychotherapists believe that the very collection of data from mentally-ill patients is an invasion of their privacy and interferes with therapy. In connection with a nation-wide study of the demography of mental patients, Dr. Martin D. Capell of the Detroit Metropolitan Center for Problems in Living, stated that truly voluntary consent is impossible where patients are seeking free mental assistance, and further, that

> "Being coerced into revealing personal aspects of oneself is dehumanizing. It is the equivalent of being forced to undress in public...Human beings typically have strong conflicting feelings about their education, employment, level of earnings, housing and previous experience with psychiatric treatment or hospitalization, just as they do about revealing themselves bodily.
>
> "The assurance that the data will be handled anonymously is empty. In the first place, the receptionist who hears the responses is a real person. In the second place, the patient is being asked to trust some anonymous authority to look after his personal interests. This is a poor introduction to help which is intended to encourage people to defend their own interests by being given maximal power of self-determination." 64

The staff of the Metropolitan Center for Problems in Living agreed with this position and withdrew from participation in the research project.

Although, as noted, there have been few cases of unwarranted release of medical research data, the possibility does exist. In 1970, researchers at John Hopkins Medical Center began genetic screening of incarcerated delinquent boys, and a matched population of non-delinquents, to see if the institutionalized boys had a higher XYY chromosome make-up.[65] (Most males are born with two chromosomes in pair 21 which controls the development of sex characteristics. Perhaps four out of 1,000 males are borne with an "extra" male chromosome attached to that pair (XYY). There is thought to be a relationship between the extra chromosome and delinquent agressive behavior.) When word of the research project became public, the press carried suggestions from various sources that the data should be turned over to the juvenile courts, threatening the confidentiality of the research project.

Furthermore, no consent had been obtained from the parents or the incarcerated children. Under public pressure, the researchers devised some consent procedures and agreed to keep the research results confidential.

More recently in Boston, a Science for the People group challenged some Harvard University researchers who are screening newborn children for XYY make-up and then following the boys as they develop to see if behavioral or other problems develop.[66] The critics focussed on the possibility that children might be stigmatized by a record of a genetic "condition" which is in fact meaningless, and that their relations with parents might be disturbed if the parents began to see them as suffering from a genetic disorder.

In both these cases, and in other genetic research as well, the issue of patient access is complicated. Parents or the research subjects may want access to the screening results, even though researchers may not be able to explain what the findings mean. Such situations require careful counselling and researchers are not always in a position to provide it. Responding to criticism of their work, the Harvard researchers said they would tell parents that some kind of genetic irregularity had been found, but would not specify it as XYY. A very sensitive follow-up project had been established, they said. The Science for the People group replied that telling the parents about the irregularity was simply a plot to get them into the follow-up program.

SCHOOL HEALTH RECORDS

The tradition of keeping comprehensive files on students goes back to the 1920's,[67] but two relatively modern trends influence the medical content of such records. The first of these is that elementary and secondary schools have become places for the provision of public medical care. In many communities, children receive brief physical examinations, hearing and eye tests, and vaccinations in the school. In some communities, the school nurse determines which children are undernourished and should be included in the free school lunch or breakfast program. The nurse then shares her findings with the local welfare department which determines whether the child is financially eligible.[68] More recently, mass screening for sickle cell anemia has been carried out in some schools. The medical information stemming from some of these health care activities is put in the school files.[69]

The second trend is the increased frequency with which the medical model is applied to deal with the learning and behavior difficulties of children in the schools. In many schools, a concerted effort is made to identify medical conditions such as dyslexia because of its impact on early learning. Similarly, thousands of children are defined as mentally retarded or brain-damaged each year and segregated into special school programs. Most recently, some school systems have begun to define troublesome children as "hyperkinetic" or as suffering from Minimal Brain Dysfunction, and to urge parents to obtain the medical care necessary to control their behavior, or in some instances, to put pressure on parents to sign consent forms which permit the school to administer drugs to correct the condition.[70]

Over the past twenty years, the employment of school psychologists and counsellors has markedly increased. Sociologist David A. Goslin reports that more than half the schools he studied in 1968 report recent increases in the gathering of psychological data about their students.[71]

Schools vary as to whether medical information is placed in a special file or left in the student's central record.[72] In some cases, teachers comment on a pupil's medical or psychological problem in the anecdotal records that are stored along with the central record of grade reports and other teacher evaluations. In other schools, such reports are stored separately and destroyed when the student graduates. Goslin reports that 40% of the schools he studied keep health information on permanent file.[73] The fact that elementary and secondary education is substantially under local control means that storage, access and retention policies for student health data differ considerably across the country's school districts.

Several important students' rights issues are raised by the collection and use of school medical records: 1) the possible inaccuracy of medical information placed in the student's file; 2) the stigmatizing or prejudicial effect that this information--whether accurate or inaccurate--may have on the student; and 3) the possible inability of the school system to prevent health information from being released outside the school.

A major controversy about the release of student medical records outside the schools took place in New York City in 1972.[74] A New York City Health Code regulation, passed in 1963, required the city school system to submit the names of drug-addicted students to the Health Department. The school system resisted complying with the regulation, supplying instead only the number of identified heroin users in the school system.

The New York State Commission on Investigation issued a report in August, 1972 sharply criticizing the New York school system for its "negativism" and complaining that "it continued to receive these alarming reports [about student drug addiction] but did nothing about them".

The Chancellor of the New York school system countered that "Counsellors and drug-education specialists who work in the schools have expressed serious doubts to me that they could successfully obtain the confidence of students, and counsel them away from drugs while also reporting them to the central register." Finally, under pressure from the State Investigation Commission and the New York City Corporation Counsel's office, the school system capitulated. Chancellor Scribner issued a directive to all schools to turn in the names of student drug users to the Central Register.

As to the possible inaccuracy of medical data, it should be noted that much of it is contributed by non-medical people such as teachers, counsellors or administrators. A teacher may note on a school record in passing that she thinks a student is retarded or that a student has psychological problems that lead to under-achievement. The problem here is that such an ad hoc evaluation may be transformed through time and transmission into acceptance as a professional medical judgment. This issue has been sharply raised during the last six or seven years by the definition of disruptive children as "hyper-active" and suffering from minimal brain dysfunction. While the label sounds like a medical one, several critics point out that it is a syndrome that can only be inferred from observation of behavior.[75] There is no simple medical test for hyperactivity. Writing to the National Committee for Citizens in Education, a parent told of her 8½ year old daughter who had been diagnosed as mildly hyperactive in kindergarten, and now has a record of being "autistic" and "brain-damaged." Several professionals in this field have seen and tested her and agreed that this is a wrong diagnosis.[76]

Similar issues are raised in the definition of school children as "mentally retarded", which usually results in their being placed in special, often inferior, classes.[77] The consequences of being mistakenly labeled "retarded" are severe: teachers alter their notions of what the child is capable of; special classes may provide much less education than the child could in fact handle; the child's relationship with peers changes; and as a result of all this, the child's self-image can be damaged, causing very real psychological problems indeed.

But even where the judgments are accurate, its significance may be misunderstood by teachers and others who see the record. That was the fear expressed by parents about the widespread sickle-cell testing done on black children in schools.[78] A group of New Jersey parents filed a complaint with the State Board of Education which challenged the decision of the Orange School Board to have school nurses and lab technicians test for sickle-cell in the city's predominantly black schools: "...serious economic and social ramifications are resulting from the improper stigmatization of the sickle-cell trait." The parents and other commentators felt that such testing might harm already disadvantaged children because teachers might not fully grasp the fact that this trait has no medical consequences for the child at all.

Such fears about accuracy and relevance of the materials in students' files were a chief impetus to the passage of amendments to the Elementary and Secondary Education Act. Known as the Family Educational Rights and Privacy Act, the legislation for the first time gives parents and students over 18 access to elementary and secondary school records.[79] The Act has been in effect for less than a year, and it is too early to tell how widely parents and students will avail themselves of this new access and what effect it will have on how school records are kept.

REHABILITATION AND SOCIAL WELFARE PROGRAMS

Local, state and federal government are undertaking an increasing number of rehabilitative and social welfare programs that involve medical records. Two such programs--treatment of drug addicts and child abuse registries--illustrate the ongoing controversy about how many records should be kept and to whom they should be disclosed.

Drug Addict Centers

It is not surprising that law enforcement agencies are keenly interested in drug addicts, and the records kept on them at drug treatment centers.[80] The cost of maintaining a heroin habit for one day is estimated at between $40 to $150. This means that the average addict (who does not have independent means) must steal up to three times the cost of his habit, since he can usually sell what he steals at no more than a third of its value. It is estimated that between 30% to 50% of all crime is drug-related.

On the other hand, medical experts stress that drug addiction is a disease and can be cured only through mental health treatment.[81] The most common technique is to provide medical and moral support during withdrawal, and then to administer a heroin substitute such as methadone in stable dosages over protracted periods while providing medical care, psychiatric treatment, and job and family counselling. Part of the treatment is the establishment of a confidential relationship between therapist and addict.

As the director of one methadone clinic put it: "The entire effort made in treatment and rehabilitation would quickly be frustrated if "treatment" appeared to be nothing more than a law enforcement technique aimed at identifying and harassing those who seek help...Without the confidence and trust established by insuring confidentiality, those who need help most will not ask for it."[82]

Mistrust in promises of confidentiality was the main reason for the failure of the armed forces' massive effort to deal with military drug abuse.[83] The mistrust was well founded. To encourage participation in its drug treatment program, the Service promised that drug abusers who volunteered for it would not be punished for possession or use, or given less than honorable discharges. But according to testimony at Senate hearings in 1972, many servicemen who sought help for their drug problems received none. Instead they were processed for administrative discharges as drug abusers.

Government agencies supporting methadone maintenance clinics sometimes wish to examine patient records for other than law enforcement reasons. The Food and Drug Administration charged, for example, that a clinic in New York was failing to determine whether its patients were heroin-addicted when they applied for treatment.[84]

The clinic, the FDA claimed, was thereby creating methadone addicts out of non-heroin users. Clinics in California were charged with encouraging patients to secure methadone from three or four different clinics by refusing to submit the names of their patients to a central register.[85]

According to a survey of 172 Methadone Maintenance Clinics, a third of the states have laws requiring that a physician file a report whenever he treats an addicted patient and nearly all of these laws require the patient's identity.[86] Four states specify that the reports must be held in confidence; two states require them to be confidential except to health and law enforcement agencies; in two states they are open to general inspection; and in the rest of the states, confidentiality of the records is not mentioned.

Most of the states with drug reporting laws keep centralized state-wide drug-addict registries which, in addition to patient identities, contain personal data gathered from physicians and treatment programs. Local and state agencies that fund drug-treatment programs may collect additional information. One drug abuse program director complained to the Pennsylvania Council on Drug and Alcohol Abuse that "This program has consistently protested demands made on it by the Allegheny County Mental Health and Mental Retardation Program to supply them with confidential information concerning our patients...It was necessary for this program to refuse to accept funding from (the County) in order to protect the confidentiality of our clients..."

A heated controversy about San Francisco's methadone maintenance program involved all of the local state and federal agencies who fund drug treatment programs.[87] The local agency, with the support of the Mayor, made its medical records available to the state agency which funded the program on a matching basis with the federal government. But the local agency removed the patients' names from the records, except for the patients referred to treatment as an alternative to prison.

The state charged that removing the names was in violation of federal guidelines and ordered the clinics closed. The local agency appealed directly to the Federal Food and Drug Administration which finally agreed to accept the records without the names. But the state remained adamant that the patients' names must be supplied. As matters stand now, the clinics are closed for refusal to comply, and state legislators are introducing bills to amend the State's Welfare and Institutions Code to end the requirement that methadone clinics' patients' names must be supplied to the state.

A similar controversy arose in Massachusetts, in connection with the Federal government's Client-Oriented Data Acquisition Process (CODAP).[88] In this program, in return for federal funding, local drug programs must provide the following information on participants: birth date, sex, race, zip code, first two initials of mother's given name, first two initials of mother's surname. The information could be interfaced with several lists, among them the Social Security Administration's files or a state's vital statistics bureau to produce the name and address of any participant within 30 seconds. Both the Governor of Massachusetts and the Mayor of Boston refused to authorize supplying this information for drug patients in the Boston are and declared they would forego the federal funding rather than comply. Again, the federal government made a special exception and said it would not cut off funding if the patient records were not identified.

According to the survey, methadone treatment centers in states with central drug registries complained of problems of maintaining confidentiality 50% more often than centers in states without such registers. The information sought by central registries included drug, criminal and medical history, social and demographic data, prior drug treatment and employment data. Moreover, the centers complained, "information in government...files frequently finds its way into the hands of police or of private credit bureaus or other businesses."

As to the physical security of the records within the 172 centers surveyed, 95% of the centers keep them under lock and key and protected by a sign-out procedure for authorized personnel. Only a third of the centers use the additional protection of assigning numbers to files instead of patients' names.

Child Abuse Registries

Recently cited statistics estimate that one American child in 500 dies of child abuse. The states have been responding to the growing incidence of child abuse for some years. Between 1963 and 1967, every state in the Union and the District of Columbia enacted a child-abuse reporting statute which required physicians and other health professionals to report suspected child abuse.[89] In the past eight years, thirty states have established central child-abuse registries to which any person may report a suspected case of child abuse.[90]

One of the chief purposes of the central registry is to attempt to identify parents or guardians who are involved in multiple episodes of suspected child abuse. Abusing parents often seek to conceal repeat episodes by bringing the child to a different clinic or health center for treatment each time.

The federal government also maintains a national child abuse registry in Denver at the National Center for the Prevention of Child Abuse which operates under the auspices of the Office of Child Development of HEW. The thirty states with central registries send unidentified records to the National Center for statistical studies.

Most of the legislation establishing central registries does not deal with the questions of access by accused parents or guardians, or the confidentiality of the material in the registers. The typical statute simply mandates the creation of a registry to which any citizen may make a report, and there is no barrier to these registries being shared with law enforcement agencies, the courts, social service agencies, welfare departments, etc.

Seven states impose varying degrees of confidentiality on the records, and the New York statute does permit access by parents or guardians after allowing the Department of Social Welfare ninety days in which to make an investigation.[91] After that, the parents or guardians must be informed of what has been said about them, but they are not told the name of their accusers. The accused are entitled to a hearing with due process protections, and if the accusation against them cannot be documented, they have the right to have the entry about them deleted from the registry. This is the only state statute with an access and deletion provision.

According to Alan Sussman, Director of the Juvenile Justice Standards Project of the American Bar Association, "child abuse" is a loosely interpreted term. A further concern is that the registries serve only to stigmatize the parents or guardians, often by totally unsubstantiated gossip; the state has little capacity, once it gets information on child abuse to provide care for the abused child or counselling for the abusing parents.[92]

CONCLUSIONS

Secondary uses of medical data raise the sharpest clash between society's interest in protecting medical confidentiality and its interest in a wide variety of other important functions, both private and governmental. In each area we examined in this chapter, a rational case could be made for every exception to the normal rules of medical privacy and confidentiality. Sometimes we saw the decision to override confidentiality traditions embodied in the law, through legislation, administrative ruling or court decision. These legally sanctioned exceptions tend to legitimate those other exceptions which have developed simply as a matter of organizational practice.

There are, however, two important recent social forces that operate to call these exceptions to confidentiality into question. The first is the movement for social change during the past two decades which has created outspoken constituencies for racial and sex equality, cultural and sexual diversity, political dissent, consumer rights, and the rights of such stigmatized groups as ex-mental patients, persons in psychotherapy, women seeking abortions, etc. These groups view the use of health criteria in decisions about employment, education, credit, government benefits,etc. as a device to reinforce restrictive social judgments about non-conforming social behavior. The debates such critics initiate over "privacy" are often really challenges to the way that conventional society confers its rewards and favors among the population.

The second social phenomenon is the deepening distrust of government that marks our era, not only among the forces for social change, but in the general population. This cynicism and distrust of the government's willingness and ability to protect confidentiality may sometimes overshadow the public's approval of many of the secondary uses of medical data treated in this chapter. In an era of confidence in the government's good word and fair play, these secondary uses would rarely stir significant public concerns. Given the harsh realities of the late 1970's however, any discussion of secondary uses of personal medical data must begin with a recognition of this public distrust, and a realization that it underlies the growing discussion of whether existing laws and controls over medical data uses are sufficiently protective of citizen rights.

FOOTNOTES

1. *Life Insurance Fact Book*, 1974 (New York Institute of Life Insurance, 1974,), p. 21.

2. Albert A. Foer, "The Personal Information Market," reprinted in *Fair Credit Reporting Act-1973*, Hearings before the Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs, U.S. Senate (U.S. Government Printing Office, 1973), p. 723.

3. *Fair Credit Reporting Act- 1973*, *op*. *cit.*, p. 461.

4. Foer, *op*. *cit.*, p. 723.

5. *Life Insurance Fact Book*, 1974, *op. cit*., p. 95.

6. Lawrence Ross, "Pathology Reports and Autopsy Protocols: *Confidentiality, Privilege and Accessibility*," *A.J.C.P.*, Vol. 57 (1972), p. 206.

7. Department of Transportation, H.U.D., *A Study of Assigned Risk Plans* (Washington, D.C., 1970), pp. 1-3.

8. *Ibid*, p. 4.

9. As reported in *The New York Times*, "Study Finds Insurers Exclude Millions Without a Sound Reason," December 3, 1974, p.66.

10. *Fair Credit Reporting Act-1973*, *op*. *cit*., p. 521.

11. Murray Weinstock and Jacob I. Haft, "The Effect of Illness on Employment Opportunities, *Archives of Environmental Health*, Vol. 29 (Aug. 1974), p. 83.

12. *Report*, American Psychiatric Association Task Force on Confidentiality, (Washington, D.C. 1972).

13. Weinstock and Haft, *op*. *cit*., p. 83

14. *New Jersey Civil Liberties Reporter*, "Matter of Lee," (November, December,1974-January, 1975), p. 7.

15. As reported in *The New York Times* (August 2, 1975), p. 70.

16. Harold M. Rush and James K. Brown, "The Drug Problem in Business," *The Conference Board Record*, Vol. 8, #3 (March, 1971).

17. *The Investigation and Suitability Programs of the U.S. Civil Service Commission*, Bureau of Personnel Investigations, (Washington, D.C., 1969), p. 8.

18. Philip Solomon, Susan T. Kleeman and William J. Curran, "Confidentiality in Psychiatric Screening for Security Clearance," *American Journal of Psychiatry*, Vol. 27, #11, (May, 1971).

19. *Anonymous* v. *Kissinger*, 499 F. 2d 1097 (D.C. Circuit, July 5, 1974).

20. "Procedures for Requesting Deletion of Abbreviated Separation (SPN) from Discharge Document," memo (mimeo) from Lawyers Military Defense Committee, ACLU Foundation (Washington, D. C., 1974).

21. *Fair Credit Reporting Act-1973*, *op*. *cit*., p. 886

22. *Retail Credit of Atlanta, Ga*., Hearings before Subcommittee of the Committee on Government Operations, House of Representatives, 90:2, May 16, 1968 (U.S. Government Printing Office, 1969).

23. *In Re Retail Credit Company*, Federal Trade Commission, Docket No.8954 (February 21, 1974).

24. Testimony of W. Lee Burge, Subcommittee on Consumer Credit of the Committee on Banking, Housing and Urban Affairs, U.S. Senate (October 23, 1975).

25. This discussion on industrial medicine is taken from the book, *Expendable Americans* by Paul Brodeur (New York: Viking, 1974).

26. For a general discussion of state licensing requirements, see Benjamin Shimberg, Barbara F. Esser and Daniel H. Kruger, *Occupational Licensing and Public Policy*, Final Report to the Manpower Administration, U.S. Department of Labor (Princeton, N.J.: Educational Testing Service, 1972).

27. Loren Siegel, "The Story of Henry Mercer," *Civil Liberties in New York*, Vol. XVII, No. 8 (Dec. 1969).

28. As reported in the Detroit *Free Press*, "Action Line," January 9, 1972, p. 1A.

29. Siegel, *op*. *cit.*, p.8.

30. Final Draft, *Proposed Rules and Regulations*, Maryland Motor Vehicle Administration, June 6, 1974.

31. For a description of the National Driver Registration Service, see *Federal Databanks and Constitutional Rights* (Part III, Vol. 4), Subcommittee on Constitutional Rights, Committee of the Judiciary, U.S. Senate (U.S. Government Printing Office, 1974), pp. 2455-2511.

32. See the discussion in the chapter on primary health providers, Zone 1, *supra*.

33. Emanuel Hayt and Jonathan Hayt, *Legal Aspects of Medical Records*, (Berwyn, Ill.: Physicians' Record Company, 1964).

34. Thomas J. Scheff, "Social Conditions for Rationality," *American Behavioral Science*, Vol. 7 (March, 1964), pp.21-27.

35. Alan F. Westin and Michael A. Baker, *Databanks In A Free Society*, (New York: Quadrangle Books, 1972), pp. 40-41.

36. Victor J. Teichner, Working Paper for A.P.A. Conference on"Confidentiality of Health Records," November, 1974, *op*. *cit*.

37. P.F. Slawson, "Patient-Litigant Exception. A Hazard to Psychotherapy," *Arch. Gen. Psychiatry*, 21: 347-351, Sept. 1969.

38. This issue was raised by a number of participants in the November 1974 A.P.A. Conference on the Confidentiality of Health Records, *op*. *cit*.

39. In Re Lifschutz, 2 Cal. 3d 415, 467 p. 2d 557 (1972).

40. *Caesar* v. *Mountanos*, Appeal brief, U.S. Court of Appeals, Filed Sept.20,1974, No. 74-2271, 9th Circuit.

41. Hayt and Hayt, *op*. *cit*., p. 156ff.

42. *A Guide for Cooperation with Communications Media*, (Chicago, Ill., American Hospital Association), no date.

43. Project interviews with newsmen in the Greater New York area. For the Bernstein and Woodward account, see Carl Bernstein and Bob Woodward, *All The President's Men* (New York: Warner Paperback Edition, 1975),pp. 55-56 and 139-140, 347.

44. As reported by Murray Schuman, "A Blighted 'Affair' Led to Bank Holdup,", New York *Times*, August 24, 1972.

45. Aryeh Neier, "Informed Voluntary Consent and Patient Access to Records," Advance working paper prepared for A.P.A. Conference on the Confidentiality of Health Records, November, 1974, *op*. *cit.*

46. Dennis Helfman, et al., "Access to Medical Records," *Medical Malpractice*,*op*. *cit*., Appendix Volume, p. 179.

47. *Ibid*.

48. See Profile of Los Angeles County Medical Center, this Report, *infra*.

49. R.G. Nathan, "The Scope of Confidentiality Issues in the Modern Medical Setting," unpublished paper, University of Pennsylvania Law School,

50. Washington, D.C. schools, for instance, station police officers in high schools where there has been a high incidence of theft or violence, according to a long-time former school board member.

51. See the Mutual of Omaha Profile, this Report, *infra*.

52. *People* v. *Newman*, 32 N.Y. 2d 379, 298 N.E. 2d 651 (N.Y. Ct. App. 1973).

53. See the Kaiser-Permanente Profile, this Report, *infra*.

54. As reported in the New York *Times*,April 23, 1972, p.25.

55. *Statistical Abstract*, 1973, p. 68.

56. National Committee on Vital and Health Statistics, U.S. Public Health Service, *Epidemiologic and Medical-Care Research*, (Washington,D.C.: National Center for Health Statistics, 1969).

57. As reported by Bernard Gauzeer, "Tests 20 Years Ago Peril Families Today," *Associated Press*, August 29, 1972.

58. Jay Katz, *Experimentation with Human Beings* (New York, Russell Sage Foundation, 1972), Chapter 1.

59. *Ibid*, Chapter 13.

60. William J. Curran, "The Tuskegee Syphilis Study," *New England Journal of Medicine* 289: 730-31, October 4, 1973.

61. *State* v. *Junker*, 482 P. 2d 775 (Wash. 1971).

62. See for example, American Hospital Association, *Medical Record Departments in Hospitals*, *op*. *cit*.

63. "Draft of Proposed Model State Law on Psychotherapeutic Confidentiality," memo prepared for the A.P.A. Conference on Confidentiality of Health Records, October 14, 1974, by the Mental Health Law Legislative Guide Project, Washington, D.C.

64. *Psychotherapy Bulletin*, April, 1970.

65. This account is taken from materials assembled in Katz, *op*. *cit*., pp.341-346.

66. As reported in the *New York Times*, November 15, 1974, p. 10.

67. David A. Goslin and Nancy Bordier, "Record-Keeping in Elementary and Secondary Schools," in Stanton Wheeler, (Ed.), *On Record: Files and Dossiers in American Life* (New York: Russell Sage Foundation, 1969, pp.29-66).

68. Florence B. Robin, *Their Daily Bread: A Study of the National School Lunch Program* (New York: Committee on School Lunch Participation, 1967), p. 23.

69. Tabitha Powledge, "The New Ghetto Hustle," *Saturday Review of Science*. (February, 1973) pp. 38-47.

70. Lester Grinspoon and Susan B. Singer, "Amphetamines in the Treatment of Hyperkinetic Children," *Harvard Educational Review*, Vol. 43, #4 (November, 1973), pp. 515-555.

71. Goslin, *op*. *cit*., p. 58.

72. One source of variation here is whether psychological test results and evaluations are regarded as "medical" records.

73. Goslin, op. cit., p. 48

74. As reported in The New York Times, August 14, 1972, p. 1, and August 16, 1972, p. 39.

75. Donald Cohen, et. al., "Mental Health Services," in Hobbs, (Ed.), Issues In The Classification of Children: Vol. II, pp. 101-102.

76. Letter from a parent, quoted in Children, Parents and School Records, The National Committee for Citizens in Education, Columbia, Md., 1974.

77. Jane R. Mercer, Labeling the Mentally Retarded, (Los Angeles: University of California Press, 1973).

78. Powledge, op. cit.

79. P. L. 93-380, 1974, Title II, Sec. 513, Elementary and Secondary Education Act.

80. Robert M. McNamara, Jr., and Joyce R. Starr, "Confidentiality of Narcotic Addict Treatment Records: A Legal and Statistical Analysis," Columbia Law Review, Vol. 73, 1973.

81. Ibid, p. 1579 .

82. Ibid, p. 1583 .

83. Ibid, p. 1584 .

84. As reported in the New York Times, Nov. 22, 1975, p.33.

85. McNamara and State, op. cit., p. 1588 .

86. Ibid, 1594 .

87. Curry v. Brian, Complaint filed Jan.9, 1974, Superior Court of California; Letter from Dr. Curry to Dr. Brian, December 31, 1973.

88. Computerworld, August 15, 1973, p. 1.

89. Alan Sussman, "Guidelines for Legislation: Child Abuse and Neglect Reporting," Juvenile Justice Standards Project of the Institute of Judicial Administration, Inc. of the American Bar Association, Sept. 1974.

90. Ibid.

91. Ibid.

92. Ibid.

Part Two
Enter the Computer

225-346 O - 76 - 8

CHAPTER 4. TRENDS IN COMPUTERIZATION OF MEDICAL DATA

INTRODUCTION

Part One documented how widely medical (and pseudo-medical) information is now distributed throughout the organizational settings of American society, and noted the main civil liberties issues involving medical data that had already come to the fore by the time computerization spread to the health care field. Having laid down these pre-computer baselines, we turn now to the automation of personal medical data.

Computerization in health care is expanding in response to the same general stimuli that have made automation attractive in other sectors of American society. These include: rising demands for private and government services by customers and consumers; demands for faster data transmission; the heavily increased paperwork necessary to satisfy such transactional demands; the rising costs of clerical labor; and increased government reporting and auditing requirements to satisfy social accountability.

These pressures, plus some special ones, are present in health care. A dramatic example of the escalating demand for services in the health field is the increase in annual hospital admissions: from 10 million in 1940 to 21 million in 1955 and then 35 million in 1974. This rise in patient demand for services comes both from the well-to-do and from the indigent who are now covered by various new governmental payment programs. In addition, there is a broadened scope to medical treatment, born of advances in drug therapy, operative procedures, and medical technology; greatly increased paperwork required from doctors and health institutions for repayment purposes; increased reporting requirements for fiscal auditing, quality-care assurance and public health purposes; the high cost of physician and paramedical time in meeting such record-keeping and reporting requirements; and most recently, the growing impact of various legal duties, ranging from documentation of procedures to avoid malpractice liability to recent judicial decisions requiring mental health institutions to prove they are furnishing adequate care to their patients. All of these functions--plus others--create an enormous, ever-increasing data-handling operation. Studies within hospitals estimate that from 25% to 40% of hospital activity is devoted to collecting, recording, communicating, and reporting medical information.[1]

In tracing how computers have been used in health care, it is helpful to recall some overall trends in organizational computer usage during the past fifteen to twenty years.[2] The basic pattern has been for automation to move first into an organization's financial activities (payroll, accounts receivable, etc.) where personnel had previous experience with electric accounting machinery and where the data being processed was of a highly routine, fixed character. Computer system developers moved next to automate large-volume, frequently used files containing data on clients, customers and subjects that was easily abbreviated and "objective" in nature. The goal here was to replace expensive clerical labor who were performing repetitive tasks, with the additional hope that services could be improved at the same time.

Many organizations moved in the 1970's beyond computerization of routinized operations and into automation of more narrative, specialized files, attracted by the prospect that more sophisticated computerization would improve the quality of decisions by line officials or by managers (a prospect strongly encouraged by vigorous marketing from the computer industry). Recent years have also seen efforts by some organizations to develop more integration of their various personal data files, through multi-file databanks and management information systems. Here the objective is to provide a comprehensive information system for management, and even to reorient major aspects of the organization's structure and procedures around the "total" information system.

On the whole, this general progression in computer utilization has been the pattern in the health care field. In describing that pattern, we have focused on the first two zones of our three zone model--primary health care and the activities of service payers and quality care assurance. This will be followed by six detailed "case histories" of Zone 1 and Zone 2 organizations that are actively engaged in computerizing personal data files. Automation in Zone 3 is so extensive and so variegated that it would take a separate study to describe computerization in law enforcement, government welfare and social service programs, employment, education, etc. Although it is not necessary to describe the entire range of computerization trends in Zone 3, we will treat the development of government health agency activities in planning and program oversight, since this rests so heavily on calls for health data to be furnished by Zone 1 and 2 organizations. The way in which automation of other Zone 3 organizations creates demands for health data from individuals or health providers will be treated in detail in Part Four, the section devoted to analyzing how computerization is affecting citizen rights in health data.

ZONE ONE: PRIMARY HEALTH CARE PROVIDERS

There are almost as many schemes for classifying primary health care providers as there are professional organizations doing the classifying. For our purposes, it is useful to organize a survey of computer applications here under three main headings:

A. Doctors' offices, small clinics and small health centers, generally with ambulatory or out-patient practices.

B. Hospitals and larger clinics and health centers, both in-patient and out-patient services.

C. Other primary health services, such as corporate health departments, prisons, nursing homes, etc.

A. Doctors' Offices and Small Clinics/Centers

An estimated 80% of health care over 900 million patient visits in 1973--is delivered in the practitioner's office.[3] While there has been no national survey of EDP use by individual or group practitioners, Daniel Harris of the American Medical Association's Department of Computer Systems in Medicine estimates that between 10% and 15% of these practitioners are now using some form of EDP.[4] This assumes use by about 2% - 5% of sole practitioners and perhaps 20%-25% of physicians in larger group practices.

Most of this computer use in offices is done by contracting with organizations offering service bureau operations to doctors. These include bureaus sponsored by local or state medical societies, commercial firms specializing in medical data processing, general data-processing service bureaus, and bank and insurance company computer services. Generally, these are batch-processed operations, with input forms sent from the doctor's office by messenger or mails to the bureau for processing. Only a few firms offer doctors on-line medical billing and administrative reporting services, where the input is made to the service bureau's central computer directly from a terminal in the physician's office.[5] A very small minority of doctor's offices have their own computers and a complete data processing system on the premises.

By far the most common computer application for doctor's offices is billing and accounting, with office-administration and claims-reporting features increasingly "hung onto" these systems. A study by the American Medical Association found only a minority of office computer-users pursuing more clinically oriented applications; the most common of these are computerized patient histories, automated multi-phasic health testing, computer-assisted diagnosis, medical records, scheduling, ECG analysis, and laboratory analysis.[6] In addition, some doctors--probably in the hundreds--have developed computer applications geared to their practice specialties or individual research interests, mostly by obtaining computer time and file storage from a university hospital system or a service bureau.[7]

One leading-edge effort to stimulate computer use in the doctor's office was a federally-funded (HEW) project conducted between 1971 and 1974 by the consulting firm of Bolt, Beranek, and Newsman, at a cost of $1.1 million.[8] Called CAPO (Computer Aids in the Physician's Office), this venture placed terminals in a group of 13 physicians' offices, linked by telephone line to a central computer operated by Meditech, Inc. Bolt, Beranek and Newsman provided software programs, orientation, and instructional training to the physicians and their staffs.

The computer applications furnished by CAPO included automated medical history, both for general screening and various specialties; diagnostic consultation; paramedical support; patient education and family health planning; and administrative services (billing, patient scheduling, etc.). When the project ended, four of the 13 participating offices indicated they would continue the computer services at their own expense. Inside and outside evaluations of the project agreed that some practitioners liked the system (where it responded to problems they felt to be important) but others did not find the system particularly helpful. The costs of hardware and software as of 1974 were such that only physicians seeking innovation in their office routines would be likely to adopt such a service, but expected reductions in cost would probably make such systems more attractive in a few years.

Citizen Rights' Aspects of EDP in Doctors' Offices

We noted three trends in doctors' office computer use that affect citizen rights. First, the main purpose--and effect--of adopting an automated health screening, patient history, and patient profile system is comprehensiveness. Doctors we talked to said that the range of subjects covered, including physical and emotional state, family history, social situation, and any economic, political or other stress-producing factors relating to medical problems was far greater than they typically obtained with patients previously. In addition, where a doctor in the "jot-it-down-on-a-5-by-8-card" era would have recorded only the most pertinent information, often in a half-legible notation useful for the doctor's own needs, automated patient records now produce detailed personal histories that can be read by all the personnel in the office.

Second, the presence of such detailed records creates a major evidentiary resource for insurance companies, workman's compensation investigators, and others involved in civil litigation involving claims. These records offer a patient-elicited declaration of conditions at the time the history was taken, plus the results of various lab tests, examinations and further interviewing that are part of the record in a multi-phasic, continuous history. Thus, automated patient screenings and histories are increasing the scope of data collection in doctors' offices, the centralization of data from different reporting sources, and the potential set of claimants who ask to see such records.

Finally, where outside EDP services are being used, an important factor is the spread of personal medical information to service bureau employees. The very fact that a well-known person has visited a particular practitioner (especially one who is a psychiatrist, or a cancer specialist) can be highly sensitive, and thus the disclosure that Citizen A is being billed by Doctor B could be a significant violation of medical confidentiality. Beyond this is the fact that some medical billing services do put substantive information on their statements, if this is the way the doctor gives it to them or if the standardized "billing package" calls for it. Service bureaus are well aware that confidentiality and security of the data entrusted to them is vital to their business success, and various kinds of personnel and security protections are used in these operations. However, some of the most celebrated breaches of security for confidential business data have taken place in service bureaus during the past decade, and the movement of personal medical data to this location clearly represents a new risk to confidentiality.

Future Prospects for EDP in Doctors' Offices

Spokesmen from medicine and the computer industry expect the use of computers in doctor's offices and small clinics to move slowly but steadily upward in the next five years. They cite the increased exposure to computers that physicians receive as they treat their patients in hospitals; courses in medical schools about administrative and clinical uses of computers; the current trend toward greater group rather than solo practice, creating more practice units for which computers could be cost-effective; and the funding of various projects(such as CAPO) by federal health agencies to develop tested applications and encourage greater EDP use in doctors' offices. Possibly the most important factor is the rapid price decline that is taking place in computing services, as small-system computers and minicomputers move into monthly costs for business data processing that many physicians are finding attractive.[9]

B. Hospitals, Clinics and Health Centers

The most recent national survey of computers in hospitals was conducted in late 1974 by the American Hospital Association.[10] Questions on computer use were sent to the Association's 7,108 member hospitals. Of the 5,912 hospitals (83.2%) that responded, 3,364 (56.9%) reported they were purchasing out-of-hospital computer services, while 1,441 (24.4%) reported having their own in-house computer. (In 1970, a survey by the Hospital Financial Management Association reported that 42% used outside EDP services and 19.2% had in-house computers.)[11]

The size of the hospital is the chief factor affecting in-house computer use. Only 7.4% of the hospitals having 6-24 beds have their own computer, compared with 55.3% of hospitals with 400-499 beds and 43.2% of hospitals with over 500 beds. Size does not determine the purchase of out-of-hospital EDP: 40.2% of hospitals with 6-24 beds buy computer services, compared with 48.2% of hospitals with 500 beds and over.

Of the hospitals that buy outside EDP services, the AHA survey found the most common applications to be business and financial (37.1%) and professional audit (17.2%). Electrocardiogram analysis (11%) was the next most frequent, with dietary, radio-therapy planning, "other clinical," and "other non-clinical" among the remaining activity.

The survey asked hospitals with one or more in-house computers about the kinds of applications being used in each of ten major departments--nursing, laboratory, pharmacy, radiology, admitting, dietary, medical records, personnel management, out-patient/emergency, and intensive care/cardiac care. The responses showed that the single most frequent computer use was for budgeting and statistical reporting, and that such use was spread quite evenly through these departments (ranging from 13.6% to 17.5%). All other applications combined in each department ranged from a low of 3.5% to a high of 9%.

In terms of equipment, 684 hospitals (11.6%) have large computers (defined as costing more than $100,000). 1,017 (17.2%) have mini-computers (defined as costing from $10,000 to $100,000) and 402 hospitals (6.8%) have remote terminals. 260 hospitals (4.4%) report they have both mini and larger computers. Use of terminals increased with the size of the hospital, from 2 hospitals having 6-24 beds, to 148 hospitals with over 500 beds. The use of terminals in hospitals has increased dramatically since this survey was conducted in 1974. One estimate is that between one and two thousand hospitals now have remote terminals.

These survey results reflect the general pattern of computer use found by the National Academy of Sciences' study to mark the rapidly changing world of computer, communications and microform technologies during the past three decades. In each field of business, government, and associational activity, there are a few organizations whose managerial style, resources, competitive position, and technical competence lead them to become leading-edge users. They are the first to try new hardware and peripheral systems as they come out, to attempt ambitious software applications, and to risk organizational change and "people problems" in these efforts. Some leading-edge users are highly successful (measured in terms of fulfilled expectations, realistic costs, etc.). Others--possibly a majority of the pioneers--are satisfied with enhanced prestige as willing experimenters, rather than being able to show truly cost-effective operations. (Computer experts have coined the phrase, "The early Christians get the hungriest lions...")

A second type of computerizing organization is the *mainstream* user. These tend to be more cautious, willing to wait until new equipment and applications are tested and proved by others, or else to make relatively guarded initial adoptions ("We do things in a modular, step-by-step way here; the 'big bang' isn't our style.") In any field, this is where the great majority of computer users are to be found.

Finally, most fields have their *low-users*, those who do some computerized data processing but are well below the mainstream average in their area. Sometimes this is a matter of size, resources, or the particular function within the field that the particular organization performs. But it may also be a general management resistance to computers on ideological grounds; fears of reaction by clients, customers or subjects toward automation of particular information functions; or resistance by influential groups of professional, middle-management or line employees toward the introduction of computers beyond a limited payroll-personnel/check-writing level.

The hospital field fits this pattern closely. During the past decade, a small number of American hospitals, perhaps 25-30, have attempted to develop applications leading toward the goal of unified or "total" computerized hospital information systems.[13] (When asked by the AHA survey whether they have a "computerized hospital information system," 275 hospitals (4.7%) say they do, and 395 hospitals (6.75%) say they "plan" to have one. No one using the term "hospital information system" in its usual meaning of integrated files, common data base, and comprehensive software can take such declarations seriously. As Collen and other authorities have stated, there are *no* such systems in operation today, nor is their appearance imminent.)[14]

Possibly a hundred other hospitals have pursued new applications in particular areas beyond the mainstream financial and administrative uses, as with various clinical and ancillary services, multi-phasic screening, on-line patient histories, in-house research, medical education, medical audit, and the like. As successes have been achieved in some of these areas, the systems have been shared or marketed, and have entered mainstream status.

Low users are probably a larger percentage of the hospital community than in many other fields. The majority of hospitals today are medium and small sized institutions and are still limited either to financial and reporting applications supplied by service bureaus or small computers with software packages supplied by computer manufacturers.

Special Features of Hospital Computerization

Some aspects of hospital automation bear directly on citizens' rights and deserve special attention.

1. Patient-Record Application

Only a minority of hospitals with in-house computers or which use outside EDP services have automated their stored patient medical records. Some of these users have patient-history and multiphasic screening programs, and some have developed automated records based on the problem-oriented medical record developed by Dr. Lawrence Weed.[15] Most of these are for ambulatory rather than in-patient uses.

2. Hospital Information Systems

As noted above, there are currently no full-dress hospital information systems (HIS), although a small group of American hospitals is working toward developing them.

Among them are: Kaiser-Permanente and El Camino Hospitals in California; Massachusetts General in Boston; the Harvard Community Health Plan; and the Texas Institute for Research and Rehabilitation in Houston.[16] In psychiatric institutions, HIS-oriented hospitals include the Institute for the Living in Hartford, Connecticut; Walter Reed Army Medical Center in Washington, D.C. and other institutions using the Computer-Support-in-Military-Psychiatry project; the Fort Logan Mental Health Center in Denver, Colorado; the Connecticut Mental Health Center in New Haven, and other institutions using the Multi-State Information System for Psychiatric Patients, developed at the Research Center of Rockland State Hospital in New York; and hospitals participating in Missouri's Standard System of Psychiatry project.[17]

What distinguishes these HIS projects is their commitment to creating a single and unique patient identification number and concentrating in one central record the data from all the patient's past and present hospital and out-patient service contacts, including (if present) psychiatric data. The goals of such unified record-keeping are both medical and administrative: to make possible the most complete and informed diagnosis of health problems and evaluation of treatment, and to generate the data base from which to improve in-house administration, claims reporting, professional review, and basic medical research. The very richness of the patient records in an HIS system underscores the citizens' rights issue--how securely will the data be kept from those within the institution who have no need to see it (e.g. limiting psychiatric data in general hospitals) and from those outside payers, quality-care reviewers, and secondary-data users who may demand access to HIS patient files.

3. Government Hospitals

In its 1974 survey, the AHA included 361 federal hospitals, 1,438 state and local government hospitals, and 4,113 private hospitals. Comparing trends in computer use showed:[18]

Type of Institution	Uses Computer Services	Has In-House Computer
Federal hospitals	53.5%	16.6%
State and local government hospitals	51.2%	23.9%
Non-Government, not for profit	63.0%	31.1%
Non-Government, for-profit	60.5%	12.6%

These figures show that computer use by government hospitals falls between the higher-use not-for-profit private institutions and the lower-use for-profit institutions. However, trends in government hospital computerization require special attention because of the sheer size of government health programs. At the federal level, for example, the Veterans' Administration hospitals are the largest medical organization in the United States, with 171 hospitals, 200 clinics, 5,500 full time physicians and 21,000 nurses. In 1975, they serviced 1.1 million veterans, with 15 million out-patient visits and almost 30 million prescriptions.[19] To the VA system, one must add the hospitals maintained by the U.S. military for service people and their dependents, the U.S. Indian Health Service, hospitals for the Merchant Marine, and special federal health institutions. Along with the hospitals maintained by municipal, county and state governments, this puts a very large part of the nation's hospital beds and hospital admissions under government auspices.[20]

The analytic literature on computerization in government hospitals shows that automation patterns do not fit into any neat "government" versus "non-government" categories; the leading-edge, mainstream, and low-user patterns in hospital computerization are distributed about as evenly in government hospitals as elsewhere.[21] However, enactment of privacy legislation affecting government agency files, such as the Federal Privacy Act of 1974 and similar Acts in four states as of early 1976, means that government hospitals will be the first affected by such new legal rules.

4. Miscellaneous Health Programs

Automation has also moved into a number of other health care activities. Automated Multiphasic Health Testing Centers are now found throughout the country, independent of hospitals, with well-known firms such as the Life Extension Institute and the American Health Foundation offering this as an off-the-street commercial service. The patient record that is generated is given to the patient or his/her physician, but a copy is kept by the screening center, much as income tax preparation firms keep copies of the returns they prepare for clients.[22]

Another recent development is the wallet-sized medical history card or "medal" that individuals can carry or wear wherever they travel. Some of these feature machine-readable patient data strips while others have microfiche forms that can be put into readers in a health care institution. Such personal medical information includes allergies, drug sensitivities, cardiac readings, conditions such as epilepsy, and other matters that would affect treatment if an individual is seized with a health emergency away from home. Several million individuals now use these portable medical-record devices.[23]

Still another computerized area is that of local blood banks, both the community-run non-profit agencies and the commercial blood banks.[24] Here, the acquisition of patient medical histories, the testing and coding of blood characteristics, managing inventories, and the creation of files matching patient identities carefully with donor history and blood code have prompted considerable use of automated systems. The American Red Cross has initiated a national, computerized Donor Deferral System, with patient identities included, designed to minimize the dangers of transmitting hepatitis by blood and blood product uses.[25]

CITIZEN RIGHTS ISSUES IN HOSPITAL EDP

1. General Changes in the Patient Record

As in doctor's offices, computer use in hospitals is changing the nature of the patient's file. In many hospitals in the pre-computer era, record-keeping was hit-or-miss, and though lots of paper accumulated in the record, these documents were often in disarray, without any indexing or current summary. Now, while the *character* of personal information that is being collected for automated patient records is not different from what was recorded before, the automated personal data are being *more systematically collected*, *more fully recorded* and *more centralized* in permanent files. Patients processed through automated history-taking are systematically asked to disclose the full range of physical, social, family, emotional and other personal data, and the resulting detailed patient profiles become a regular feature of the file, updated steadily as the patient remains with that care provider.

From a health care standpoint, this is one of the most desirable features of automation--patient records are full, up-to-date, easily understood and are linked together from various departments and previous episodes. From a civil liberties standpoint, however, this trend means that all the medical and paramedical personnel in a facility who have access to the computerized files now have more detailed personal data and more comprehensive social histories than in the typical manual system, except for psychiatric facilities.

In addition, computerization of patient data is facilitating (and is sometimes directly intended to facilitate) the sending of some automated patient data to organizations outside the primary care sector--to service payers and those charged with quality care assurance, and to the Zone 3 users such as public health agencies, welfare and rehabilitation programs, licensing authorities, judicial authorities, employment-insurance evaluators and so forth. Much of the computer-based information activity in these zones depends on automation of data bases in the hospital for timely and complete input. The further automated the hospital data are, the easier, cheaper and more rapidly Zone 2 and 3 organizations can call for production of what they want. Automated centralized patient records not only mean greater ease of transmission at a lower cost, but also the availability of far more detail in the medical record than has been the case in the past. This means that these records will require not just the observance of traditional standards of care as to confidentiality (uneven as those have been) but a new definition of legal and public-policy boundary lines for data-sharing, and the creation of monitoring and enforcement machinery to police the boundaries.

2. Privacy Issues

We have observed that when individuals seek medical help, they willingly reveal the most intimate aspects of themselves to the health professional; collection of such data is clearly relevant to treatment. Revealing financial or family data may be less acceptable, but even here, the justifications for requiring disclosure are strong.

However, as we noted in Part One, there are issues as to what should be recorded and for how long it should be preserved, as in the case of the San Francisco women who sought to have hospitals return the "psychiatric-need" letters written by their doctors to justify abortions before the 1972 Supreme Court ruling. We did not learn from the ACLU attorney handling this case whether there were any coded notations in computerized files about the letters, or whether they were only kept in the manual files. But the problem of what is to be recorded in computerized records is likely to be an increasing problem, as illustrated by a letter from a pediatrician who practices in a large metropolitan hospital:[26]

The computerized records, she wrote, were "incalculably valuable for both information retrieval, scheduling of appointments, etc. But it poses terrible problems in our treatment of adolescents. What do I do when a youngster tells me she is sexually active? I need to retain this information to assure the problem is dealt with in some manner. What about drug use (illicit)? What about negative attitudes towards parents or school? A missed menstrual period and possibilities for pregnancy? I need to record these matters, but am deeply distressed about their availability to anyone on the computer (and we have had some bad experiences in this line).

"I have been considering a bipartite record; the first is available to anyone needing health information and is not compromisory data in any way; the second is "confidential" data and either not stored in the computer at all (but kept in a separate confidential drawer) or if stored only available to one or two key people. But this is difficult to work out."

We see this as a Zone 1 issue because if the stigmatizing information were not preserved in the files of the primary health provider, the problems of ancillary and secondary uses would be eliminated or greatly lessened. If primary health providers insist on preserving everything for legal, research, or administrative purposes, we can expect considerable conflict over the increasingly rich and detailed files accumulating in hospitals, health-care plans, employer medical records, and school and university medical files, especially in the automated "total patient information systems"

Also a privacy matter is the issue of whether a given automated system has informed patients that their medical data is being automated, and how it will be used.

3. Confidentiality Issues

When they reveal intimate personal data to health professionals, patients expect these to be kept "confidential," following the ethical and legal norms commonly understood to attach to the doctor-patient relationship. We have already discussed how widely identified patient data are now disclosed for Zone 2 activities and for many secondary governmental and private uses noted in Zone 3, including releases of information to the press, to law enforcement, and to commercial reporting agencies that raised serious confidentiality issues, generally because there were no clear legal controls over such data-sharing.

Because detailed medical records are still kept in manual files in primary health care, this is where improper or disputed leakages of personal health data are still centered. The same management policies, doctor's ethics or hospital cooperation with outsiders that made these disclosures possible could take place from automated medical files in the future as these come to be repositories of more detailed patient files. Thus, the citizens' rights issue is to see how securely the more detailed and "richer" automated records can be secured against such misuse.

4. Patient Access to Records and Medical Information

Traditionally, as we have already discussed, the medical profession has maintained that the doctor should decide what the patient should know about his/her condition, treatment, or prospects. Records in health care facilities have been considered by law to be the property of the institution, and patients normally have been able to inspect their records only by bringing a lawsuit for negligence and getting a court order authorizing access. In recent years, consumer and patients' rights groups have championed the right of patients to see their records if they wish and to have them explained by the doctors where the notations are not intelligible to laypersons. These same access disputes arise when personal medical data are placed in automated files; where no duplicate manual files remain, the right of a patient to get a printout of his or her record will be the basic issue.

Future Prospects for Hospital Computerization

Hospitals have not used computers as extensively as many other industries, such as banking or insurance. A survey in 1970 reported that after a decade of automation in hospitals, "55% of all hospital information processing applications are still performed by hand,"[27] and this figure has not been substantially reduced today. The relatively low use of computers is reflected in the sales figures. One study reported that sales of hospital computers in 1974 were only $156 million,[28] even though American hospitals spend between 7 and 10 billion annually (between 24-33% of their annual budgets) to acquire and communicate information.[29]

Studies of hospital automation are in agreement about the causes for low EDP use here.[30] The major factors have been: resistance by medical practitioners and allied health professionals; the high costs and disillusioning failures of early, widely-heralded hospital EDP projects; uncertainties of funding for venturesome efforts, and an absence of strong federal commitment in this area; and a lack of clear "systems concepts" around which to organize the files and flows of information. The last problem is seen as stemming as much from conflicts within the medical profession and among medical planners as to the ways to reshape health-care delivery as it has been the failure of systems experts to develop good systems models of the medical milieu **as** it really operates.

However, recent marketing studies have been highly optimistic about the future of EDP use by hospitals. One study predicts hospital computer sales will go to $380 million by 1979.[31] More specifically, the marketing forecasts predict: much wider use of remote terminals to capture medical data where it is generated; a surge in the use of small in-house computers among smaller hospitals (75-300 beds); wide use of computerized hospital management systems supplied by various manufacturers and services on a "turnkey" basis (installed and ready to use); and a growth in multi-hospital associations or data-management plans that will make use of shared data processing facilities.

Many academic and medical-professional analysts reach similar conclusions about the bright future of computer use in primary care. Dr. Marion J. Ball, director of the computer systems and management group at Temple University's Health Sciences Center divides hospital computer systems today into two levels.[32] Level I is focused on data collection and message-switching capabilities (administrative data processing) and does not "maintain an electronic patient medical file." Such systems now cost approximately $1 to $2 per patient-day. Level II systems "maintain a complete computerized patient medical record during the patient's hospital stay, and are programmed to handle clinical information as well as requisitions." Such systems now range from $2.50 to $9 per patient-day, depending on how many clinical applications are in the system. Using Dr. Ball's classification, Dr. Stanley E. Jacobs, former director of the division of computer systems of the American Hospital Association, predicts the following: "By 1980 I anticipate that at least 50% of all short term general hospitals over 200 beds will have installed at least a Level I hospital information system. By 1985, I expect a majority of these hospitals will have Level II..."[33]

Not all the experts agree that hospitals are approaching a major take-off point in computer usage--at least not in the near future. At the conference held to discuss a preliminary draft of this report,[34] several experienced observers of computerization in primary care emphasized that hospital computer uses so far represent a stitching together of bits and pieces of separate applications. What has been lacking is the development of a conceptual model of information priorities and uses in the hospital, especially a model that could be generally accepted by doctors and other health professionals and by the patients, not just by health-care planners, hospital business managers, and data processing technicians.

Until such a professionally-acceptable and patient-regarding model is developed, through a basic rethinking of organizational goals, professional rewards and roles, and man-machine relationships, many experts feel that computer use in hospitals will remain oriented to administrative data processing and limited clinical programs, rather than moving toward larger information systems of integrated files and patient-record data bases. Those taking this view believe that even the infusion of large amounts of money for developing hospital information systems--something that has not been present in the 1965-1975 decade--would not lead to significant breakthroughs in the near future. Even passage of national health insurance would not make a major difference, in this view, since such a system would almost certainly operate through limited data reporting systems, and would not compel hospitals to develop comprehensive information systems.

One of the reasons for the divergency of predictions about more sophisticated use of computers in hospitals in the future is the lack of agreement about their value and cost-effectiveness in the present. Most observers agree that computers have helped hospitals and health centers meet the crush of paperwork in patient billing, accounting, claims processing and administrative reporting. They also agree that computer applications in perhaps a dozen areas of clinical use have improved the delivery of services and have been cost-effective. Beyond these areas of agreement, however, the effects of more ambitious information systems are difficult to measure with anything approaching scientific rigor, or even marketplace criteria. While some interesting efforts have been made to evaluate the effects and costs of particular hospital information system projects, a recent conference on the evaluation of health information systems concluded that there was little agreement today on the terms and procedures for such evaluations, and that it may be too early in the evolution of such projects for evaluation to be more than experimental and tentative.[35]

Because our study deals with the impact of computer use on citizen rights, and is not a study of the effectiveness of hospital computerization on health care, we did not attempt to make a national estimate of how hospital information system projects are doing. We did look to see how the activities of a sample of such leading-edge systems are affecting individual rights, and this appears in our profiles in Part Three.

C. Other Primary Health Services

As we noted in Part One direct health care is provided in a considerable number of institutional settings today other than doctors' offices, hospitals, and public health centers. Automation has spread deeply into some of these other locations, which include college student health services, corporate medical programs, nursing homes, prisons, school nurse and emergency offices, and similar facilities. We will look at one of these college health services, to show how automation is being used in such facilities.

There are about 2,500 colleges and universities in the United States, with some 7 million students in attendance. The institutions usually provide health services for resident students ranging from in-patient emergency care to regular medical, dental, and mental health services with full time staffs of doctors, nurses, and other medical personnel. Typically, colleges obtain a medical history from the entering student; maintain a regular patient medical record during the course of the student's matriculation, and keep special files for drug and alcohol abuse data, birth control and abortion data, suicide episodes, psychiatric care, and similar matters.

Some colleges and universities have developed their own computerized patient record and administrative systems, and are much like medium-sized community health centers in their patterns of computer utilization. A few leading-edge systems, such as the Harvard Community Health Plan,[36] serving students, faculty, and staff members of the Harvard community, have pioneered in advanced applications. Particularly interesting from our standpoint are the commercial firms that market automated medical questionnaires and problem-oriented records for these purposes. For example, Medical Datamation, an Ohio-based company, offers DASH, Database Acquisition for Student Health.[37] This is a 964-item self-administered questionnaire that covers personal identification, family, and insurance items, then asks about demographics, allergies, immunizations, hospitalizations, illnesses, disability, other medical problems, operations, fractures, medications, habits and risk factors, eating, exercise, smoking, alcohol, drugs, trauma, and information or help wanted by the student. The questionnaire also asks for data on each of the main bodily systems and presents 44 questions about the student's feelings.

DASH offers a medical database report, a problem list, a problem-monitoring report, and statistical summaries, all generated from the automated data. The basic report package costs about $10 per student. The company claims that the DASH process saves colleges considerable time over traditional history taking, eliminates the need for "most pre-enrollment physical examinations" for the average student, and allows better concentration from the outset on students with problems.

The questions asked about "Habits and Risk Factors" and "Feelings" illustrate the scope of inquiry:

HABITS and RISK FACTORS

Your habits influence your ability to achieve and maintain good health and long life. Mosit of the questions on this page reflect factors which increase your risk of developing physical or emotional problems. Please answer each question realistically. You are not being "graded", and this is not a test.

EATING **Do you generally or frequently –**

	Yes	No	
500	___	___	Eat irregularly, skip meals?
501	___	___	Eat an excess of animal fats, dairy foods?*
502	___	___	Eat an excess of sugar, pastries, starches?*
503	___	___	Drink 5 or more cups of coffee per day?
504	___	___	Drink 5 or more cola drinks per day?
505	___	___	Tend to stay overweight?
506	___	___	Tend to stay underweight?
507	___	___	Eat fruits regularly, every day?
508	___	___	Eat vegetables regularly, every day?

* *An excess is a LOT, like 5 or more single servings per day of the type of food in question.*

EXERCISE **Do you generally or frequently –**

	Yes	No	
515	___	___	Get heavy exercise on an irregular basis?
516	___	___	Consider golf, bowling, archery and similar sports strenuous exercise?
517	___	___	Get some type of regular exercise?
518	___	___	Get regular strenuous exercise such as running, swimming, bicycling?
519	___	___	Do you know the type of exercise required to strengthen the heart?

SMOKING

	Yes	No	
525		___	Do you smoke a pipe?
526		___	Do you smoke cigars?
527		___	Do you currently smoke cigarettes?
528		___	Did you formerly smoke cigarettes but stopped completely?

If you have ever smoked cigarettes, specify amount and duration.

529	___ Less than ½ pack/day	533	___ Less than 1 year
530	___ ½ to 1 pack/day	534	___ 1 to 5 years
531	___ 1 to 2 packs/day	535	___ 5 to 10 years
532	___ Over 2 packs/day	536	___ Over 10 years

You're well over half done now.
The hardest part is over. Press on!

ALCOHOL

	Yes	No	
540	___	___	Do you drink alcohol?
541	___	___	Did you formerly drink alcohol but stopped?

If you have ever drunk alcohol, specify amount and duration.

542	___ Occasionally, socially	546	___ Less than 1 year
543	___ Several drinks/week	547	___ 1 to 5 years
544	___ Several drinks/day	548	___ 5 to 10 years
545	___ More than 3 drinks/day	549	___ Over 10 years

DRUGS **Do you generally or frequently –**

	Yes	No	
555	___	___	Currently use pot, speed, downers, acid, heroin or any similar drug?
556	___	___	Formerly used such drugs but stopped?
557	___	___	Know the common names and appearance of various forms of such "street" drugs?
558	___	___	Know the short and long term effects of these drugs?

If you have ever used any of the drugs mentioned above, specify which ones and how often.

	Yes	No	
559	___	___	Marijuana (pot)
560			___ Rarely
561			___ Frequently
562	___	___	Amphetamines (speed, uppers)
563			___ Rarely
564			___ Frequently
565	___	___	Hallucinogens (LSD, acid, mescaline)
566			___ Rarely
567			___ Frequently
568	___	___	Narcotics (heroin, H, morphine)
569			___ Rarely
570			___ Frequently
571	___	___	Methaqualone (Sophers, Quaalude)
572			___ Rarely
573			___ Frequently,

TRAUMA, ACCIDENTS and OTHER HAZARDS
Do you frequently –

	Yes	No	
580	___	___	Ride a bicycle on heavily traveled roads?
581	___	___	Ride a motorbike or motorcycle?
582	___	___	Ride a motorcycle without helmet and jacket?
583	___	___	Tend to exceed the speed limit while driving?
584	___	___	Drive after drinking alcohol or taking drugs?
585	___	___	Water ski or boat without a life preserver?
586	___	___	Walk alone at night in a strange neighborhood?
587	___	___	Hitchhike or pick-up hitchhikers?
588	___	___	Get exposed to very loud noises?
589	___	___	Get exposed to insecticides or dangerous chemicals?
590	___	___	Know how to swim?
591	___	___	Wear reflective clothing when walking after dark?
592	___	___	Know how to give CPR (cardio-pulmonary resuscitation, artificial respiration)?
593	___	___	Know how to give mouth-to-mouth breathing?
594	___	___	Know how to give closed chest cardiac massage?

© Medical Datamation 1975

FEELINGS *Mark the frequency with which you have the feelings or problems listed.*

M = Most of time
S = Some of time
N = None or rarely

M S N

850 ___ ___ ___ Feel sad, depressed?
851 ___ ___ ___ Feel lonely?
852 ___ ___ ___ Cry without apparent reason?
853 ___ ___ ___ Wish to end it all?
854 ___ ___ ___ Plan a way to kill self?
855 ___ ___ ___ Unable to concentrate on anything?
856 ___ ___ ___ Awaken, can't go back to sleep?
857 ___ ___ ___ Still tired after a night's sleep?
858 ___ ___ ___ Feel tense and anxious?
859 ___ ___ ___ More nervous than your friends?
860 ___ ___ ___ Worry about health?
861 ___ ___ ___ Worry about things generally?
862 ___ ___ ___ Have trouble falling asleep?
863 ___ ___ ___ Jump at sudden noises, shake badly?
864 ___ ___ ___ Have frightening, recurring thoughts?
865 ___ ___ ___ Feel calm and contented?
866 ___ ___ ___ Unusually afraid of high places?
867 ___ ___ ___ Unusually afraid of closed places?
868 ___ ___ ___ Unusually afraid of crowds?
869 ___ ___ ___ Suffer from nervous exhaustion?
870 ___ ___ ___ Get upset easily, highly irritable?
871 ___ ___ ___ More touchy than your friends?
872 ___ ___ ___ Go to pieces if you don't constantly exert control over yourself?
873 ___ ___ ___ Get angry when told what to do?
874 ___ ___ ___ Feel more violent than your friends?
875 ___ ___ ___ Get along with people?
876 ___ ___ ___ Get upset when things are not precise and orderly?
877 ___ ___ ___ Do most things on impulse?
878 ___ ___ ___ Feel it is OK to steal as long as no one gets hurt or caught?
879 ___ ___ ___ Feel overly shy, sensitive?
880 ___ ___ ___ Get feelings hurt easily?
881 ___ ___ ___ Greatly upset by criticism?
882 ___ ___ ___ Tremble or feel weak whenever someone shouts at you?
883 ___ ___ ___ Feel optimistic about the future?
884 ___ ___ ___ Get completely mixed up when you have to do things quickly?
885 ___ ___ ___ Afraid to be alone?
886 ___ ___ ___ Usually wish you had someone to advise you?
887 ___ ___ ___ Have feelings of inadequacy?
888 ___ ___ ___ Have strong feelings of dependency?
889 ___ ___ ___ Seem to be more aggressive than your friends?
890 ___ ___ ___ Have legal problems?
891 ___ ___ ___ Have financial problems?
892 ___ ___ ___ Have marital problems?
893 ___ ___ ___ Have family problems?
894 ___ ___ ___ Have sexual problems?
895 ___ ___ ___ Have questions about sexual matters?
896 ___ ___ ___ Feel someone is out to "get" you?
897 ___ ___ ___ Hear voices when no one is around?
898 ___ ___ ___ Feel someone is controlling you in an unusual way?
899 ___ ___ ___ Feel you are responsible for the sins of the world?

TESTS During the past year, have you had

Yes No

920 ___ ___ Blood count?
921 ___ ___ Blood sugar check?
922 ___ ___ Chest x-ray?
923 ___ ___ TB skin test?
924 ___ ___ Urine check (urinalysis)?

INFORMATION *Do you want further information on the following, or help with problems you may encounter in the areas described?*

Yes No

930 ___ ___ Alcoholism
931 ___ ___ Birth control
932 ___ ___ Cigarette smoking
933 ___ ___ Diet programs
934 ___ ___ Drug abuse
935 ___ ___ Emotional problems
936 ___ ___ Exercise programs
937 ___ ___ General health hazards
938 ___ ___ How to cope with loneliness
939 ___ ___ Legal problems
940 ___ ___ Marital problems
941 ___ ___ Money or financial problems
942 ___ ___ Self breast exam
943 ___ ___ Sexual problems
944 ___ ___ Venereal disease
945 ___ ___ What to do if a medical emergency occurs

CONCLUSION

Yes No

960 ___ ___ **Do you have any other problems not covered by this questionnaire?**

Please give us your opinion of this system.

961 ___ Great
962 ___ Good
963 ___ Generally good, criticism minor
964 ___ Don't like it

Please sign your name.

Signature ______________________________

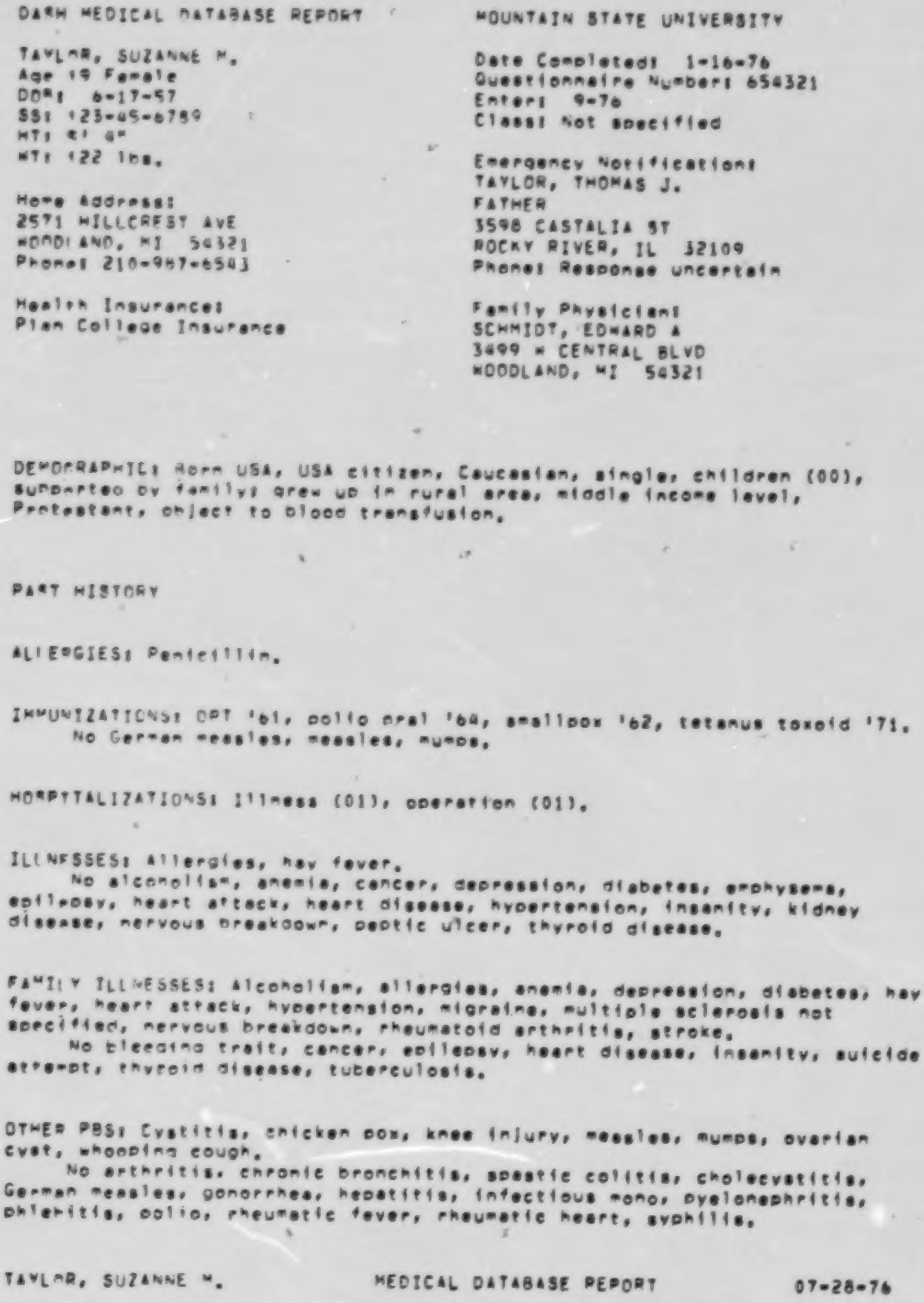
You're done!
Thank you for completing the questionnaire.
Please check back through to make sure you haven't skipped any sections or pages.

Enclose the completed questionnaire along with your check to Medical Datamation in the postpaid envelope and mail as soon as possible.

Good luck at college!

© Medical Datamation 1975

From these questions, DASH produces a Medical Database Report illustrated by the following sample on a fictitious "Suzanne M. Taylor."



```
DASH MEDICAL DATABASE REPORT            MOUNTAIN STATE UNIVERSITY

TAYLOR, SUZANNE M.                      Date Completed:  1-16-76
Age 19 Female                           Questionnaire Number: 654321
DOB:  6-17-57                           Enter:  9-76
SS: 123-45-6789                         Class: Not specified
HT: 5' 4"
WT: 122 lbs.                            Emergency Notification:
                                        TAYLOR, THOMAS J.
Home Address:                           FATHER
2571 HILLCREST AVE                      3598 CASTALIA ST
WOODLAND, MI  54321                     ROCKY RIVER, IL  32109
Phone: 210-987-6543                     Phone: Response uncertain

Health Insurance:                       Family Physician:
Plan College Insurance                  SCHMIDT, EDWARD A
                                        3499 W CENTRAL BLVD
                                        WOODLAND, MI  54321


DEMOGRAPHIC: Born USA, USA citizen, Caucasian, single, children (00),
supported by family; grew up in rural area, middle income level,
Protestant, object to blood transfusion.


PAST HISTORY


ALLERGIES: Penicillin.


IMMUNIZATIONS: DPT '61, polio oral '64, smallpox '62, tetanus toxoid '71.
     No German measles, measles, mumps.


HOSPITALIZATIONS: Illness (01), operation (01).


ILLNESSES: Allergies, hay fever.
     No alcoholism, anemia, cancer, depression, diabetes, emphysema,
epilepsy, heart attack, heart disease, hypertension, insanity, kidney
disease, nervous breakdown, peptic ulcer, thyroid disease.


FAMILY ILLNESSES: Alcoholism, allergies, anemia, depression, diabetes, hay
fever, heart attack, hypertension, migraine, multiple sclerosis not
specified, nervous breakdown, rheumatoid arthritis, stroke.
     No bleeding trait, cancer, epilepsy, heart disease, insanity, suicide
attempt, thyroid disease, tuberculosis.


OTHER PBS: Cystitis, chicken pox, knee injury, measles, mumps, ovarian
cyst, whooping cough.
     No arthritis, chronic bronchitis, spastic colitis, cholecystitis,
German measles, gonorrhea, hepatitis, infectious mono, pyelonephritis,
phlebitis, polio, rheumatic fever, rheumatic heart, syphilis.


TAYLOR, SUZANNE M.           MEDICAL DATABASE REPORT           07-28-76
```

OPERATIONS: Tonsillectomy.

FRACTURES: None.

MEDICATIONS: Antihistamine, birth control med, vitamins, other medicine(s) not listed.

DISABILITY: Permanent physical disability, pb that precludes taking PE.

HABITS AND RISKS FACTORS

DIETARY: Eats irregularly, excess saturated fats, excess coffee.
No excessive carbohydrates, cola drinks.

EXERCISE: Irregular heavy exercise, no regular strenuous exercise, lacks exercise information.

SMOKING: Smokes cigarettes, less than 1/2 pack per day, less than 1 year.
Does not smoke a pipe, cigars.

ALCOHOL: Drinks alcohol, socially, duration not specified or uncertain.

DRUGS: Cannot identify street drugs, lacks drug effect information.
Does not currently use drugs.

TRAUMA/HAZARDS: Deficient in CPR, deficient in resuscitation, deficient in cardiac massage.
Does not drive after alcohol or drug use, participate in hitchhiking, get exposed to loud noises, get exposed to dangerous chemicals.

SYSTEMS REVIEW

HEAD: No problem.
No dysequilibrium, vertigo, syncope, seizures, weakness arm(s), weakness leg(s), paresthesias arm(s), paresthesias leg(s), headaches.

EYES: No problem.
No visual pb not corrected, esotropia, exotropia, colorblindness, blindness, eye pain, diplopia, halos around lights.

ENT: Frequent rhinorrhea, frequent sneezing.
No hearing loss, earaches, sinus trouble, postnasal drip, epistaxis, hoarseness, carious teeth, bleeding or sore gums, upper plate, lower plate.

HEART AND LUNGS: No problem.
No heart valve problem, murmur, irregular rhythm, tachycardia, cardiomegaly, wheezing, persistent cough, chest pain, dyspnea.

DIGESTIVE: No problem.
No nausea, vomiting, hematemesis, melena, diarrhea, constipation, red blood in stools, indigestion, abdominal pain.

URINARY: No problem.
No enuresis, incontinence, nocturia, frequency, dysuria, hematuria, flank pain with fever, hesitancy.

WOMEN: No PAP test within past year.
No breast nodule, vaginitis, dyspareunia, frigidity, irregular menses, menorrhagia, current pregnancy.

MUSCULOSKELETAL: Joint stiffness due to injury.
No neck pain, back pain, swelling of feet or lower legs, joint pain not injury related.

OTHER SYSTEMS: Dry skin or brittle nails, intermittent fatigue.
No polydipsia, weight loss, constant fatigue, between meal weakness, rapidly growing mole, rash or pimples, hot flashes, fever or chills, pallor, swollen or tender nodes.

FEELINGS: Sadness or depression - S, loneliness - S, tenseness - S, more tense than friends - M, worries generally - S, feels calm and contented - N, compulsive - M, highly sensitive and shy - S, more aggressive than friends - S.
No suicidal desires, trouble falling asleep, frightening recurring thoughts, irritability, violent feelings, impulsiveness, sensitivity to criticism, gross inadequacy, gross dependency, sexual problems, feelings of persecution, audio hallucinations, delusions.

TESTS-PAST YEAR: No chest x-ray, TB skin test.

INFORMATION: Exercise programs, health hazards, self-breast exam, medical emergencies.

ADDITIONAL PHS: Section not marked.

OPINION OF SYSTEM: Section not marked.

Reviewed by

The issues raised by the use of such automated history programs as DASH were highlighted in a communication our project received from a nurse who is serving on the privacy committee of a state medical records association. She commented:[38]

"It is my opinion that the program DASH is a problem in the area of automation of student medical information. First of all, the questionnaires are compiled into a problem list - it seems that DASH places in this problem list any 'Yes' checked by the student in the questionnaire, including such things as information requests for birth control or emotional problems. What qualifies these as 'Problem areas'?

"In addition, the Problem Monitoring Report strongly violates privacy and confidentiality. In the questionaire, the student is not told that such reports will be compiled, nor is the student told who will have access to the reports (faculty, counselors, etc.). The Monitoring Report could be particularly harmful in a student health service where often times non-professionals are employed, and who might disseminate the information to unauthorized persons. The sensitivity of the data compiled in the DASH program indicates to me the potentially harmful effects of such a program."

A special problem of citizen rights posed by the growing automation of data in the direct-care facilities of colleges, corporations, penal institutions and the like is that the doctors and other medical personnel in these settings are employed by organizations that exercise authority over the individuals receiving the medical care--as educator, employer, correctional agency,etc. As the volume and sensitivity of the personal and medical data in these computerized files increases--illustrated by the DASH profile--the issues of who else within the college, company, or correctional institution obtains access to these data becomes critical, as well as issues of how ancillary uses--for research, service payment by third parties, quality-care assurance--and secondary uses--licensing, law enforcement, drug reporting,etc.--will be administered.

ZONE TWO: SERVICE PAYERS AND HEALTH-CARE REVIEWERS

Service Payers

We have already described the nature and operations of the American health insurance system. As we noted, 190 million Americans are covered by private health insurance, 75% in group plans. About 51% of this business is written by commercial health insurance firms; 8% by non-profit firms; and the balance of 41% by the "Blues" (the 71 Blue Shield Plans reimbursing for doctors and office procedures and 73 Blue Cross plans covering hospitalization).

Before the passage of Medicare (1965) and the initiation of Medicaid (1966), automation of private health insurance files had proceeded actively,primarily using the "batch-processing" of first and second generation computer systems. With large policy-holder files to record, premium payments to administer, claims to process, and management reports to generate, many health insurance companies were heavy users of computers in the first decade of organizational automation.

During the pre-Medicare era, the main government involvement as a service payer came from state and local welfare departments, which bore the main burden of reimbursing doctors, nurses, and hospitals for services provided to the indigent outside of the public medical facilities.

After federal grants-in-aid to the states for such payments were initiated in the 1950's, state payments to medical vendors under public assistance welfare programs rose to $514 million by 1960.[39] This put the additional burden of information management for such payments primarily on local and state welfare agencies. Beyond the minimum financial applications, computerization was slow in unfolding in government welfare departments in the 1955-1965 era, for reasons that include the deeply-bred "hand-work and case-work" traditions of such agencies, a "Great Society" rather than management-efficiency focus in the 1961-65 phase, and the primacy of political factors in local management of welfare eligibility and distribution.

The passage of Medicare and Medicaid radically changed the automation patterns in service paying. As George A. Ryan has written, "the rapid influx of Medicare claims reached almost unmanageable proportions. Notwithstanding the computer facilities available to carriers, the data management problems which occurred as a result of Medicare legislation defied for a time efforts on the parts of many carriers to cope with the volume of claims data."[40] From 1966-67 until recently, most of the commercial, Blues, and non-profits were preoccupied with adopting third and fourth generation computer system approaches to meet these sharp rises in claims processing. For example, Blue Shield claims went from 200 million in 1968 to an estimated 1.2 billion in 1975. Today, claims processing consumes about 50% of EDP expense in health insurance operations.[41] Our profile of Mutual of Omaha in Part Three shows how one leading-edge user responded to these dynamic conditions in the past decade.

State welfare agencies were given primary responsibility for administering Medicaid (49 states set up Medicaid programs, with only Arizona not participating). While the state welfare agency determines eligibility, it has used fiscal intermediaries (the private carriers) on a contract-basis to handle payments to primary care providers. State Medicaid information management of these operations has been weak in both its administrative and oversight functions. There have been some federal efforts to develop a Model Medicaid Management system, notably with leading-edge state welfare departments in a few states such as Michigan and Maine.

The Automated Client Information System (CIS) of the Michigan Department of Social Services, under development since 1970, is worth describing here. CIS was originally conceived as one of eight subsystems for improving management of Michigan's Medicaid Program, but the system's data network has now been expanded to include information on all residents who are currently receiving any form of state social services or have received any such benefits in the past two years. The major objectives of the system are to identify and enroll individuals in social service programs; issue authorization cards for Medicaid; furnish necessary recipient eligibility information to Medicaid providers; and centralize maintenance of medical and public assistance data.

The CIS is now the largest on-line health and welfare eligibility system in the country.[42] Each of Michigan's 83 counties is linked to one of five regional communications centers by individual video-keyboard data terminals (VDT's) located in selected county offices, state offices and medical facilities and used to enter and receive information from the statewide data center in Lansing. Authorized county personnel contact the assigned-center VDT operators by telephone when they wish to submit an inquiry or update data stored in the central computer facility. Telephone security checks and electronic edits are used to maintain confidentiality.

Prior to the implementation of the CIS, Michigan's Medicaid Program lacked a reliable data base upon which to make even fundamental decisions concerning eligibility and the payment of bills. Through its on-line update capabilities, the system no longer rejects nearly 3,000 provider claims each week as it did under the old system, because of processing lags in eligibility and re-eligibility checks. The Department of Social Services also reports reduction of administrative and payment costs, facilitation of system audits, and minimization of fraud and duplication.

From a citizen rights standpoint, several trends in automation among payers and intermediaries deserve notice. As health insurance firms are accumulating automated historical files on their policyholders, the level of personal medical detail in these files has been widening. With health costs skyrocketing, insurers and intermediaries are under pressure to scrutinize claims more closely--eligibility for the service provided, whether the service is covered by the policy, whether it was medically necessary and properly provided, whether the charge was within payment guidelines, and so forth. This has led service payers to insist that "full data" be supplied: positive identification of patient and medical provider, exact medical conditions and services provided, specific medical diagnosis or condition. The advent of PSRO reviews, and the expected reviews under future national health insurance plans, create additional pressures for collecting identified, detailed, evaluative data.

Clearly the insurance function demands that some medical data be furnished to payers, not only to determine the appropriate amount of the claim but to monitor for fraud by both claimants and primary-care providers. It is this demand for detail that raises the issue of incursion into the doctor-patient relationship, especially when the medical condition involves a socially-stigmatized area or one whose disclosure could lead to loss of opportunities by the patient.

What has the extensive computer use in Zone 2 done to observance of confidentiality in service payment? So far, not much. The crucial aspect of this question is unclear policy definition, which pertains equally to manual records. Generally, charges of improper leakage of personal data from Zone 2 raise the question: Just what is a private or government employer, or other third party, entitled to know about specific medical conditions of a subscriber or claimant? Should no information at all be given to third parties on the ground that health insurance firms receive this information solely for purposes of claims adjudication? Or should group policyholders, whether government or private, be entitled to learn of certain health conditions that could impair their employees' job performance or make them ineligible for promotion or security clearances, etc. The point to underscore is that this is a gray area today in terms of law and policy, not one on which law is clear and is being willfully violated.

But while leakages of confidential medical data have so far involved manual forms, not computer printouts, there is little doubt that patient and doctor confidence in automated service payment will be impaired if imprecise policies prevail. The issue is whether service payers should be collecting and/or retaining as much data as they do now, given the fact that many medical and civil liberties commentators feel they are not limiting its circulation sufficiently in manual forms.

Another trend in automating service-payment mechanisms over the past two decades has been the entry of data processing firms as intermediaries under Medicare and Medicaid, and in various utilization review projects. Among the best known of these is the Electronic Data Systems Company (EDS) owned by H. Ross Perot, which processed over 75 million health insurance claims in 1973 for various state agencies and Blue Shield/Blue Cross plans. This lodges personal medical data still further away from the ethical constraints of the primary-care providers or the Blues (which the medical and hospital professions themselves developed and still influence directly). Given the sometimes politicized character of the contracting process that has awarded claims-data contracts to commercial firms, and the essentially non-medical character of these "data shops," attention clearly needs to be paid to how well protected these files are today in legal status and how securely they are kept in fact.

Utilization Reviews

Since health care is a complex mixture of provider institutions, payers and carriers, and health agencies, rational administration and evaluation depend on the collection of statistical data about patients--their demographic characteristics, medical problems, treatment provided, outcome, etc. Such trend data is needed to evaluate medical procedures, plan and administer individual facilities, and coordinate local,regional, or state health resources.

For these reasons, a number of medical data systems have been developed in recent decades that collect trend information through sample surveys of individuals, program-operation data by private payers or government agencies, or case data directly from primary care institutions. Such data allow institutions and planning agencies to analyze and compare patterns of care, outcome, costs, etc., and to do basic research.[43]

The most important example of such activity is the hospital discharge data system for in-patient care activity, of which there are about a dozen currently operating. The largest of these, and the only one operating nationwide, is the Professional Activity Study (PAS) of the Commission on Professional and Hospital Activities,[44] a non-profit corporation sponsored by the American Hospital Association, American College of Physicians, American College of Surgeons, and the Southwestern Michigan Hospital Council. Originally founded in 1953, PAS now collects individual case abstracts from participating hospitals (2100 in 1975, of which 1800 are in the U.S.). It provides a database used by the participating institutions to evaluate their care and utilization patterns, and produces national or regional data for baseline comparisons of many kinds.

Participating hospitals skim off from their medical records and send PAS a set of basic data about each patient discharged. This covers a coded PAS hospital identification, a patient number supplied by the hospital, no patient or doctor identity (these are kept locally by the contributing hospital), patient demographics (age, sex, and race), clinical service, date of admission, date of discharge, all diagnoses, all operations, form of admission, complications, consultations from other departments, how discharged or if died, interservice transfer, source of payment (or expected), detailed enumeration of investigations and examinations done, drugs used, other therapy, special unit care, and (as of 1974), PSRO information relating to certified admission, concurrent review, and similar matters. In addition, space on the case abstract is provided to incorporate additional optional items that a PAS participant may want to store and use, such as patient residence, type of accomodation within the hospital, and special therapy.

PAS moved into computer processing in 1961 and now has almost 110 million individual case abstracts stored in its automated database. PAS reports for participating hospitals are prepared monthly, semi-annually, and annually. These provide profiles of care for medical evaluation, practice display, medical audit materials, basic patient statistics, quality of care assessment, and similar purposes, as well as regional and national comparisons representing other PAS participants. Special options allow a hospital to get utilization and audit reports, length of stay studies, study of patient charges, and other special analyses.

There are about 10 regional hospital discharge data systems throughout the United States, such as the QUEST Program of Northeast Ohio, the Hospital Utilization Project of Western Pennsylvania, the Medical Record System of the California Health Data Corporation, and the Connecticut Utilization and Patient Information System.[45] There are also projects on ambulatory care data systems, and various special-purpose data systems covering particular diseases, health conditions, or community health center operations.[46]

The basic confidentiality principle of the PAS data system is that the hospital retains the identity of the patient and the doctor, with the case abstract filed only by a number. The participating hospital, knowing the number, can have reports drawn up on the basis of various grouping of case abstracts along any line it wishes, but PAS employees and other participating hospitals cannot obtain a case abstract with the name of a patient or doctor on it.

Quality Care Assurance

The 1972 federal legislation requiring professional standards review (PSRO) under Medicare, Medicaid, and Maternal and Child Health Programs[47] has led to the creation of a first wave of local PSRO organizations sponsored by local medical practitioners. The PSRO's obtain data from the various providers--hospitals, HMO's, prepaid medical plans, psychiatric institutions, nursing homes, etc., as well as from fiscal intermediaries--and analyze these according to quality-care criteria to be set up by the local PSRO. The data systems being developed by these PSRO organizations are automated, and will be linked to the computer systems of the providers and carriers. Basic personal data to be included in a case review are expected to include patient identification, demographic data (age, race, sex, residential area), hospital identification, dates of service, diagnostic data, procedures data, patient disposition data, identification and practice data, on attending physician, and identification and practice data on operating physician.

Our project visited several developing PSRO organizations and studied the data-system plans that they and others are implementing. From a citizen rights standpoint, basic issues here involve the disclosure of patient identity both in initial peer review and in any successive appeals that might be taken (including appeals that could place identified patient data in regional or even national review files), as well as the patient's right of access to the PSRO record.

ZONE THREE: COMPUTERIZATION OF HEALTH AGENCY FILES

We noted in this chapter's Introduction that we would not attempt to describe patterns of automation in all the industries and government activities that use health data to make various social judgments--in employment, education, licensing, credit, life and auto insurance, welfare, law enforcement, etc. What does belong in this chapter, however, is a description of several important trends in computerization by government health agencies. We are dealing here not with assurance of quality care by government (that has already been treated in Zone 2) but with the general planning, evaluation, and coordination functions performed by local, state, and federal health agencies.

Government oversight of hospitals, mental health facilities, and other health care centers is a matter of overlapping jurisdictional responsibility in the United States. Given our mixture of private-for-profit, private-non-profit, and government-owned facilities, plus the supplying of funds to local institutions by federal and state programs, there is a mixture of single-agency and cooperative-agency supervision that puts individual institutions under reporting duties to various government health agencies. Many of these duties require only statistical data, but many others call for the reporting of identified personal information about patients, and also the supervisory authorities rights of inspection that include access to personal records.

State health agencies occupy probably the pivotal position in this regulatory network, having the primary supervisory authority over local health facilities and also serving as the interfacing unit with the federal government for most local and state health-assistance programs. In a survey conducted in December of 1974,[48] the National Association of State Information Systems found that of 45 states reporting, state departments of health in 21 states computerized patient census files; 10 had patient information processing applications; 10 maintained hospital administration files; and 6 had applications for medical records. Seventeen of these state departments had their own computers, while others had services supplied by state data processing centers.

Another survey in 1974 examined computerization by state mental health authorities.[49] Out of 47 jurisdictions replying, 29 indicated they had implemented computer data systems that collected case information from local mental health centers. Twenty-three of these stored personally-identified psychiatric information in their files, either through name or Social Security number. The primary purpose for such automation was found to be the control of costs, with closer scrutiny of eligibility the key technique. Only three states--Arizona, Colorado, and Utah--collected no identifying data, while three other states reported that they were "moving away from storing identifiable information" in these files.

This survey found that "requesting affirmative authorization for computerizing a patient's personal psychiatric information is virtually non-existent." Only one state reported that local patients sign authorizations for release of confidential information to the state automated file, and another state said it obtained patient permission to file the data by Social Security number, which is the identifier used in this system. "If the client refuses to sign a release," this state said, "the [local] center assigns a pseudo-social security number to that client's data."

The citizen rights issues posed by such state health-agency automation revolve around the issue of whether such records need to be collected and stored by the state with personal identifiers. When these are attached, this raises the issue of informed patient consent to such use; notice of and control over access to the records by other state agencies (licensing authorities, welfare agencies, police,etc.); and rights of inspection by the individual patient as to what is put in about him or her. We already noted (in Part One) the fight that has erupted over the reporting of identified case information by local health and mental health facilities to state health or welfare agencies serving as administrators of Title XX funds under the Social Security Act's medical-aid programs.

One important new development in federal law deserves mention here. In 1975, Congress enacted the Health Planning and Resources Development Act, providing a major reorganization of the way that local agencies must set plans for and coordinate the use of federal assistance funds in the health field.[50] The Act terminates the existing structure of regional medical programs and comprehensive health planning agencies and calls for the creation in 1976 of 200 health service areas in the United States. Each will be administered by a health service agency that can be a private body, a non-profit organization, or a public agency, depending on local option, though it must then have in it representatives of the facilities and agencies receiving federal aid in that area. This has set off a lively struggle to see whether doctors, hospital administrators, consumers, or local health officials will dominate the new agencies, and different solutions may emerge throughout the country.

What is important for our purposes is that the act requires each of the 200 agencies to create a data base on the health status of its residents; an inventory of local health facilities, personnel, and services; the organization and operations of the area's health delivery system;patterns of utilization; the effect of that system on health; and its impact on environmental and occupational-exposure conditions. This represents perhaps the most ambitious effort to date by the federal government to develop comprehensive statistics for evaluating local health systems (both as whole units and for specific treatment problems) and to get a national picture of health conditions. Guidelines still have to be issued by HEW as to how these data systems will operate, but the issues of identified versus statistical data, controls over data circulation, and patient access clearly lie ahead.

A NOTE ON PHOTODUPLICATION AND CITIZEN RIGHTS

Though our primary focus in this Part has been on computers, we must stress that there is another important information technology that is affecting health-care records and citizen rights--photoduplication. Until the 1960's, most hospital patient records were kept as original paper documents. When third parties wanted copies of these records, for claims purposes, litigation, etc., the medical record department would abstract the relevant portions of the document, with only rare use of the cumbersome and expensive photostating method. Records were also subject to the control of sign-out and sign-in procedures. With the 1960's, xerography arrived; today, it is estimated that over 70% of hospital medical record departments own photocopying equipment, and supplying photocopies of records has become standard procedures. Microfilming also arrived in the 1960's, and as space problems became more acute and costs of microfilming went down, many hospitals put their records, especially inactive records, onto microfilm storage.

The importance of these trends in photoduplication for citizen rights is that the pressures on medical record administrators to comply with requests by service payers, insurance companies, and government reviewers often leads them to photocopy or make a microfilm print of the entire medical record, or at least an entire page, even though the information requested by a third party, or to which such party is properly entitled, may only be a portion of the patient record. The costs of locating the relevant data, masking out parts not pertinent, and explaining such procedures to the requesting parties are often more than overworked records departments can expend. In addition some medical record departments allow service payers and insurers who can show patient release forms to come to the record library and do the photocopying themselves, paying for the use of the hospital's photoduplicating equipment. Where this is done, such third parties handle the patient records themselves, and the capacity for breaches of confidentiality are increased. Also, when persons with a right to sign out records take them, the ubiquity of photocopying machines leads to an inability to control copying, and further copying from those copies.

Health records administrators have recently criticized such developments as jeopardizing confidentiality. But they note that the tremendous increases in required reporting, the shortage of staff to apply more restrictive procedures, and the widespread use of sweeping patient releases ("supply any and all hospital records...") make it difficult for the record administrators to deal with this trend on their own.[52]

SUMMARY

Computerization of personal medical information has been marked so far by haphazard growth; it has not developed according to thoughtfully conceived plans for achieving integrated health information systems within individual facilities or throughout the health care field. At the same time, policy as to the citizen rights issues of privacy, confidentiality, and access is also developing on an individual, ad hoc basis, for the most part simply carrying over into computerized files the same practices pursued with manual records. The basic concern of health care professionals, civil liberties observers, and computer experts is this: given the more detailed, more centralized, more permanent, more easily-transmissible quality of computerized medical records, the flawed procedures and policies currently employed with respect to manual records threaten to be seriously inadequate to the computer era.

FOOTNOTES

1. See statement and references in Morris F. Collen, editor, Hospital Computer Systems (N.Y., 1974), 3.

2. For a full discussion of these trends, see Alan F, Westin and Michael A. Baker, Data Banks in a Free Society (N.Y., 1972), 217-240.

3. Profile of Medical Practice, 1974 Edition, Center for Health Services Research and Development, American Medical Association, 192.

4. Telephone interview with Daniel K. Harris, Department of Computer Systems in Medicine, American Medical Association, July, 1975. This estimate was found "generally sensible" by health-marketing experts consulted at IBM, UNIVAC, and Bolt, Beranek and Newman.

5. See, for example, "On-Line System Expedites Bills for Doctors," Computerworld, July 31, 1974, S-17.

6. G.S. Ryan and K.E. Monroe, Computer Assisted Medical Practice: The AMA's Role, Center for Health Services Research and Development, American Medical Association, 1971.

7. See, for example, "Farm Area Cancer Victims Aided," Computerworld, Sept.1, 1972; and papers in Clinical Medicine and the Computer, Proceedings of the Fourth Annual Conferences of The Society for Computer Medicine, 1974.

8. Progress Report No. 2512 (1972) and Final Summary Report No. 3096 (1975), CAPO: Computer Aids in the Physician's Office, conducted by Bolt, Beranek and Newman, Inc., Cambridge, Mass., under grants from the Office of Health Care Technology, National Center for Health Services Research and Development, Health Services and Mental Health Administration. See also the project description and evaluation in Gerald A. Giebink and Leonard L. Hurst, Computer Projects in Health Care (Ann Arbor, Mich.: Health Administration Press, 1975), 122-128.

9. Harris interview, supra.

10. 1974 Special Survey on Selected Hospital Topics, Bureau of Research Services, American Hospital Association, Topic 8, Hospital Computers (1975).

11. The State of Information Processing in the Health Care Industry, Hospital Financial Management Association, 1970, 9.

12. Westin and Baker, note 4 supra.

13. The literature on leading-edge hospital computer use is becoming both extensive and introspective. Beside the flow of news articles and commentaries in general medical periodicals and computer magazines, the individual "applications briefs" on installed systems written by computer manufacturers and systems firms, and the panel papers prepared at annual medical and computer meetings, several major publications have recently appeared:
    1. Hospital Computer Systems: How to Use Computers in Medical Centers for Better Patient Care, edited by Morris F. Collen, (New York: John Wiley and Sons, 1974), a comprehensive discussion of the main efforts over the past decade, by various hospitals, to develop integrated-file, on-line information systems for medical care.
    2. Progress in Mental Health Information Systems: Computer Applications, edited by Jeffrey L. Crawford, Donald W. Morgan, and Daniel T. Gianturco, (Cambridge, Mass.: Ballinger Co., 1974), a similarly detailed and critical discussion of leading-edge efforts in the mental health field.
    3. Gerald A. Giebink and Leonard L. Hurst, Computer Projects in Health Care (Ann Arbor, Mich.: Health Administration Press, 1975), a survey of general trends in health care computerization and reports on 29 leading-edge applications, conducted in 1973-74 by Health Care Management Systems under a grant from the Robert Wood Johnson Foundation.

4. Safeguarding Psychiatric Privacy: Computer Systems and Their Uses, edited by Eugene Laska and Rheta Bank, (New York: John Wiley and Sons, 1975). This volume uses the Multi-State Information System for Psychiatric Patients developed at Rockland State Hospital, New York, as the basis for a wide-ranging discussion of automated mental health systems, their uses and limitations, and the patient rights issues involved.
5. Proceedings of MEDINFO, 1974, The First World Conference on Medical Informatics, Stockholm, August 5-10, 1974, a collection of wide-ranging, multi-national reports on hospital and health-care automation developments and issues.
6. Clinical Medicine and the Computer, Proceedings of the Fourth Annual Conference of the Society for Computer Medicine, New Orleans, Louisiana, November 7-10, 1974, available through the Society for Computer Medicine, Edina, Minnesota, focusing primarily on clinical uses by the office practitioner and in health institutions.
7. The Journal of Clinical Computing, a bi-monthly publication of "international, interdisciplinary" focus on "areas related to automation of health data," the various volumes on Computerization of Clinical Records, and the publications of the Buffalo (New York) Medical Society's Joint Task Force on Ethical Data Systems, all of these under the editorship of E.R. Gabriel, Buffalo, New York.
8. Computers and Medicine, a bi-monthly newsletter published by the American Medical Association, edited by Daniel K. Harris, of the AMA's Department of Computer Systems in Medicine. A Special Report was also recently issued (1974) by the AMA in cooperation with the Association of Data Processing Service Organizations): "Survey of EDP Services Offered the Medical Community by Data Processing Service Organizations."
9. Specialized survey reports and studies. Recent examples include Marion J. Ball's, "Medical Data Processing in the United States," in the January, 1974 issue of Hospital Financial Management (Vol.28, No.1, 10-30); Jane H. Murnhaghan's, "Health-Services Information Systems in the United States Today," in the March 1974, New England Journal of Medicine (Vol. 290, 603-610); and Paul A. Bonner's, "Data Processing Systems for Medical Care Appraisal," in Barry Decker and Paul Bonner (editors), PSRO: Organization for Regional Peer Review (Cambridge, Mass.: Ballinger Co., 1973).
10. Marion J. Ball, How To Select a Computerized Hospital Information System (Switzerland: S. Karger, 1973).

14. Collen, Hospital Computer Systems, note 1 Supra, vii and Chapter 1.

15. Weed's basic publication was Medical Records, Medical Education, and Patient Care (Cleveland: Case Western Reserve Univ., 1969). He has a popularly written and updated description of his approach in Lawrence L. Weed, Your Health Care and How to Manage It (Burlington, Vt., PROMIS Laboratory, Univ. of Vermont, 1975). See also John C. Bjorn and Harold D. Cross, Problem Oriented Practice (Chicago : Modern Hospital Press, 1971) and J. Willis Hurst and H. Kenneth Walker (editors), The Problem Oriented System (N.Y.: MEDCOM, Inc., 1972).

16. For Kaiser, Massachusetts General, and Texas Institute, see the chapters on these systems in Collen, Hospital Information Systems, note 1 supra; for El Camino, see the series of reports by El Camino staff delivered at Medinfo, 1974, note 13 supra. On Harvard Community Health, see Norma Justice, G. Octo Barnett, Robert Lurie, and William Cass, "Development and Implementation of a Medical/Management Information System at the Harvard Community Health Plan," 1974 Proceedings of the National Computer Conference, 159-165.

17. These systems are treated in Crawford, Morgan, and Gianturco, note 13 supra.

18. Note 10, supra.

19. "The V.A.: A Massive Turnaround," Government Executive, Feb., 1975, 28-29.

20. As noted later, such government hospitals are the ones being affected first by passage of general privacy legislation.

21. This conclusion is supported by the common experiences reported by the governmental and non-governmental systems in Collen; Crawford, Morgan and Gianturco; and MEDINFO, 1974, all *supra*.

22. See M. Collen, "Automated Multiphasic Health Testing" and K. Soghikian, Preventive Health Maintenance Clinics," in Collen, *Hospital Information Systems*, note 1 *supra*. Also, "Special Issue: Automated Multiphasic Health Testing," *Journal of the American Hospital Association*, Vol. 45 (March, 1971); "Test Center Provides Health Profile," *Computerworld*, Aug. 2, 1972, 21; "Prospective Medicine: A Health Forecast," (Life Extension Institute), *Pastimes*, Dec., 1974.

23. See "Portable Medical Records May Save Your Life," New York *Times*, Feb.21, 1974.

24. For one well-described system, see "System/3 at King County Blood Bank," IBM Application Brief, CK 20-0653-0.

25. F.R. Ellis, L.I. Friedman, B.F. Wirak, M.J. Hellinger, W.S. Mallen, and T.I. Greenwalt, "A Computerized National Blood Donor Deferral Register," *Journal of the American Medical Association*, Vol. 232, No.7 (May 19,1975), 722-724.

26. Communication to this Project, November, 1975.

27. Hospital Financial Management Association, note 11 *supra*.

28. *The Medical Computer Industry*, Creative Strategies, Inc. San Jose, California, 1975.

29. Marion J. Ball, "Computers: Prescription for Hospital Ills," *Datamation*, September, 1975, pp.50-51.

30. See note 28 *supra*, as well as: *Health Industry DP*, Frost and Sullivan, New York, N.Y., 1975, and *EDP For Hospitals: New Directions for Survival*, Quantum Science Corp., New York, N.Y. 1975. The scholarly literature voicing such judgments can be found in the works by Collen, Crawford et al., Giebink and Hurst, and Ball in note 13 *supra*.

31. Note 28 *supra*.

32. Ball, note 29 *supra*.

33. *Ibid*.

34. See description and attendance list in the Introduction to this Report.

35. Russell C. Koza, *Health Information Systems Evaluation* (Boulder, Colorado: Colorado Associated University Press, 1974).

36. See note 16 *supra*.

37. *The DASH Medical Questionnaire*, Copyright, Medical Datamation, 1975.

38. Communication to this Project, October 1974.

39. Robert Stevens and Rosemary Stevens, *Welfare Medicine in America* (N.Y.,1974),23.

40. George A. Ryan, "Data Management Under Professional Standards Review Organization (PSRO)," in *Socioeconomic Issues of Health, 1974*, Center for Health Services Research and Development, American Medical Association, 70.

41. Estimates from IBM health industry marketings personnel.

42. "Description of the Client Information System," Department of Social Services, State of Michigan, November, 1973.

43. Murnaghan, note 13 *supra*.

44. "The PAS System," Commission on Professional and Hospital Activities, Ann Arbor, Michigan, 1973, 1974, 1975; issues of the PAS Reporter, 1974; Telephone interview with Vergil N. Slee, President, July 26, 1974.

45. These are fully described in Bonner, note 13 *supra*.

46. *Ibid*.

47. Public Law 92-603, the 1972 Amendments to the Social Security Act.

48. *Information Systems Technology in State Government* Report by the National Association of State Information Systems (1975).

49. Verne B. Kelley and Hanna B. Weston, "Computers, Costs, and Civil Liberties," *Social Work*, Vol. 20, No.1, Jan.1975, 15-19.

50. P.L. 93-641. See also Joel Harnett, "A New Law To Manage Our Health Economy," *Government Data Systems*, Dec. 1975-Jan. 1976, 11-15.

51. Interview with Gus Stuhldreher, Xerox Medical Marketing Division, Dec. 18,1975.

52. Letter from Prof. Elaine O. Patrikas, chairman, Department of Health Records Administration, Temple University, Oct. 17, 1975.

Part Three

Profiles of Computerizing Organizations

225-365 O - 76 - 10

INTRODUCTION

Having mapped the general trends in computerization of medical data, we turn now to profiles of six organizations currently involved in automation projects. These are:

1. Los Angeles County Medical Center;
2. Martin Luther King Jr. Health Center, in New York City;
3. Kaiser Permanente Health Plan, Oakland, California;
4. U.S. Indian Health Service;
5. Mutual of Omaha Insurance Company;
6. Multi-State Psychiatric Information System, in Rockland County, New York.

Our purpose in presenting these case studies is to explore how organizational factors, especially choices as to health-care goals and administrative philosophies, are shaping both the utilization of computer technology and the consideration of citizen rights.

As to computer utilization, producing detailed profiles is important because the deployment of computing and communication resources is still essentially a matter of organizational artistry, not management science. The development of computer systems requires managers to exercise choice in selecting the files and data flows to automate, arranging configurations of hardware and terminals, writing software, defining operator-machine relationships, setting patterns of data-sharing inside and outside the organization, deciding on levels of organizational monitoring and reporting, and choosing the type of individual consent and patient access, if any, that data subjects will be given. Understanding such choices is greatly aided by analyzing how real organizations have approached such matters during the past decade.

From a citizen rights standpoint, the importance of doing profiles lies in tracing how issues of privacy, confidentiality, and individual-access were treated by these organizations before they moved into automation; how computer use has affected those practices; how on-going changes in American law and social norms are affecting management practices; and what problems and issues of citizen rights are currently unfolding in these organizations, or can be seen looming ahead as computerization expands.

Four of these organizations are primary-care providers in our Zone 1 category; one is a Zone 2 private health insurer; and the sixth is a Zone 3 research organization.

While it is impossible to reflect all the significant variables among health-care organizations in six profiles, we have tried to include most of the important ones. The following chart gives a preliminary overview of these:

CHARACTERISTICS OF PROFILED ORGANIZATIONS

ORGANIZATION	CLIENTELE	OWNERSHIP	TYPE OF COMPUTER USE	QUALITY OF HEALTH CARE OR SERVICE	TREATMENT OF CITIZEN RIGHTS	LIKELY PROSPECTS IN COMPUTERIZATION
L.A. COUNTY HOSPITAL	Urban Poor, Minorities	Public, County	"Mainstream"	Good Emergency Facilities, Average For Other Services	Fair To Weak	Continued Mainstream
MARTIN LUTHER KING CENTER	Urban Poor, Minorities	Private, Federal-Funded	"Mainstream"	Good and Innovative	Good To Excellent	Continued Mainstream
KAISER HEALTH PLAN	Middle-Class, and Unionized Workers	Private, Non-Profit	Advanced	Excellent and Innovative	Good	Continued Pioneering
INDIAN HEALTH SERVICE	Rural Poor	Public, Federal	Advanced	Innovative But Weak In Outcomes	Fair	Future Uncertain
MUTUAL OF OMAHA INSURANCE	Primarily Middle and Upper Class, Some Lower-Middle.	Private, Profit	Advanced	Innovative and Strong As Insurer	Good	Continued Advanced Use.
MULTI-STATE PSYCHIATRIC INFORMATION SYSTEM.	Multi-Class, in Different User Facilities	Public, State	Advanced	Innovative In Systems-Development Work.	Good	Probably Continued Pioneering

To develop the profiles, our project reviewed patterns of automation with marketing experts from three computer manufacturers. We also collected published descriptions of over 150 organizations. Once we had made our selections, we wrote to the organizations describing our project and asking to do a site visit to them.

After materials about each organization had been assembled and studied, a team of staff members visited the organization during 1974 and 1975, usually for an initial visit of 2 days with follow-up visits and telephone calls as needed. A draft profile was prepared and sent back to each organization so that facts could be checked and policies further explained. Updating of developments for all six organizations was done through February of 1976. The organizations' managers were not asked to approve the descriptions or judgments presented; what appears here represents the views of the project teams who did the initial write-ups, and the project director, who did the final revisions and rewriting.

After each profile, we have made some observations about the key citizens rights issues posed by the health-care philosophy and computer usage of that organization. These serve as flags for our main policy discussions and recommendations, which are saved for the last chapter of this report.

CHAPTER 5. LOS ANGELES COUNTY MEDICAL CENTER

The Los Angeles County Medical Center serves the urban poor. Like many other governmental institutions in the city, it struggles against the burdens of underfinancing, personnel shortages, overcrowding, and a medically-harmful physical and social environment. In terms of citizen rights, it is part of the current urban governmental system, one more institution that has come under attack for infringing upon peoples' rights in the name of doing them good or providing them with social services. While not among the most advanced computer users, Los Angeles has been developing a patient data bank that was planned to bring significant improvements to patient care and education. How its computer use, and its general administrative policies, affect citizen rights will be the focus of our profile.

Background

Medical Center is part of the Los Angeles County Hospital system, which serves the 500 square miles of the city and its surrounding municipalities. It dates back to 1878, when it was begun as the Los Angeles County Hospital and Poor Farm, with a 100 bed facility. Today, with any of the county's 7 million residents legally entitled to reserve care, the system has nine county hospitals and eleven outpatient clinics and rehabilitation centers, as well as 62 clinics run by the Community Health Service. In fact, most of the county patients are poor and members of racial minority groups; those who cannot afford either private physicians or private health plans. Only for emergencies (such as auto accidents) and for specialized care (communicable diseases) does the County system serve the middle class as well.

The Medical Center is composed of four hospitals*in East Central Los Angeles, with beds for 2,000 patients. It is a huge complex: over 90,000 patients admitted a year and 850,000 outpatients. It employs more than 1,000 interns, residents, and full time physicians; 70% of these are interns and residents from the University of Southern California Medical School, with which the center is affiliated as a teaching institution. The center also has 1,800 nursing personnel and over 5,000 other health workers. The labs complete more than 7 million test measurements each year, including more than 1,400 X-rays every day. About 20,000 surgical procedures are performed in a year. In 1975, the center's budget was approximately $300 million.

The Los Angeles County System, like many local-government hospital systems, has been criticized in recent years for not providing adequate care and for showing insufficient respect for patients' dignity in processing them through the hospital. In 1970, for example, a group of interns and residents charged that lack of care at the Medical Center had resulted in unnecessary patient deaths and injuries.

---

*General Hospital, Women's Hospital, Pediatric Pavilion and Psychiatric Hospital. The total inpatient admissions for Los Angeles' nine hospitals in 1974 was almost 200,000 and over 1.8 million outpatient visits. It has over 2 million square feet of hospital space and a total staff of 3,000 physicians, 2,000 students, 2,000 nurses, and 8,500 employees.

The County Hospital Commission investigating the charges concluded that they were exaggerated, but acknowledged that serious patient care problems did exist. More recently, a study commission found that while the general level of care was adequate, it was not evenly distributed throughout the county, and discouraged people in poor areas from securing the kind of routine care they need. Criticisms of fiscal mismanagement have also been raised. Hospital officials respond that the County Hospital system has corrected the problems cited by its staff, and does a good job considering how severely funds are limited to it. They also maintain that its administration is basically good, and better than at most municipal or county hospitals. Both hospital physicians and the system's critics agree that *emergency* care at the Medical Center is excellent.

The County hospital system has a budget of approximately $300 million. Less than 10% of this comes from out-of-pocket payments by patients or the private insurance coverage they pay for. The remainder comes from taxpayers, either through direct County support or state and federal programs such as Medicare and MediCal. In recent years, the hospital has felt increasing pressure from the County to pass the costs of care on to individual patients or to state and federal programs for which they are eligible, and this, as we will see, has affected computer uses there.

Computer Development at Los Angeles Medical Center

Between 1962 and 1966, several studies of health information system possibilities for the Los Angeles area produced plans for a pilot data bank project at the Los Angeles Medical Center. An on-line admissions system went into operation there in late 1968, and was adopted by the county hospitals by 1970.

The project had four objectives at this point: (1) to capture all patient data and utilize the system primarily for patient care and research rather than the more usual financial and administrative objectives; (2) to develop the problem-oriented medical record pioneered by Dr. Lawrence Weed; (3) to develop a MedicAlert system to flag by terminal a warning of pre-existing conditions whenever a patient's record was called up; and (4) to provide the basis for linking the Center's medical data with outside health agencies for research, evaluation, and planning purposes.

Creation of a Patient Data Bank and achieving terminal communication among the nine county hospitals became the main emphases of the plan in the early 1970's, through a gradual accumulation of records and a "modular growth" of computer applications. By 1972, about half of the County's 2.5 million records were computerized, with 860,000 of the Medical Center's 1 million records on the computer. Admissions and Laboratory applications were the first to be developed, followed by a fiscal system and a pharmacy application.

Funding for the computer project has come from Los Angeles County, not outside sources. It averaged $3.5 million annually from 1968 to 1970, and about $5.5 million since 1971.

Basically, the Medical Center computer project produced computer-assistance for what is still essentially a manual record system, using paper records, shelves, file cabinets, and messenger services. To understand how this system works, we look first at the admissions process and then the use of patient records within the hospital for treatment purposes.

The Admissions Process

When a patient enters the Center, either through the emergency room or admitting area, an admissions clerk secures as much identifying information as possible: name, address, race, sex, mother's maiden name, religion, birthdate and marital status. Social Security number and driver's license number are collected to serve as back-up identifiers. If the patient already has a hospital identification, a Medicare or MediCal*card, or an enrollment card from a private insurance plan, the clerk notes the numbers.

Identification information from the Patient Information Form is then entered into a computer system via one of the video-display terminals in the admitting area. Six to ten seconds later, the screen displays a list of names, addresses and birthdates of recent past patients who most closely match the new patient. The clerk looks for a close match, and if he/she finds one, prints the information about that patient on the Application Record and makes any necessary corrections of the permanent record (e.g. change of address).

This Identification system contains more than 1½ million names. Roughly 40% of the in-patient admissions are identified as having previously been to a county hospital facility. If the patient is not identified as having been a previous County patient, the clerk calls the identification section of the Medical Records Department and gets a new record number for the patient.

The primary purpose of the Admissions/Identification system is to determine what individual or agency will pay for the patient's medical care. The need for an immediate determination of who will pay must be seen in the context of how the Medical Center is financed:

1. Private payment: Only 10% of the patients have private insurance or sufficient income to cover all their bills. The bills are substantial: outpatient treatment in 1974-75 was billed at roughly $30 a day plus the cost of lab tests, prescriptions and other "extras"; inpatient treatment averaged $184 a day, with surgery billed at $290 a day, intensive care $420, and psychiatry $165.

2. Medicare/MediCal: Approximately 53% of the patients are enrolled in Medicare or MediCal. The Social Services Department fills out the appropriate forms for these programs, copies of which go to the agencies involved. The patient is billed for any deductible portion that is not covered by these agencies and the agency is billed for the rest.

3. County Support: Approximately 35% of the patients are not enrolled in either a federal or state program and claim they cannot afford to pay out of private insurance or their personal income. The funds to support the care of these patients come from the tax revenues of Los Angeles County.

There is strong pressure from the County to reduce its 35% support by (a) identifying every possible patient who is eligible for either state or federal aid, and (b) collecting fees from all those who are ineligible and have some financial resources. The collection of identifying data upon admission and the comparison with the past hospital record is the first step in assuring accomplishment of these two ends.

---

*MediCal is California's state supplement to Medicare.

Where the patient is not covered by state or federal programs, an effort is made by a Financial Services Worker in a personal interview to find out whether the patient is eligible for either by collecting information as to his/her financial resources, including income, personal and real property, savings and other assets, which the patient must swear to and document by the production of pay stubs, bank books and other records. Patients who are eligible for federal assistance and who earn too much money to qualify for county assistance, or who refuse to provide the necessary financial information, are billed in full for hospital services, on an installment basis if necessary.

Since June of 1975, Medical Center hospitals have been tied into a commercial billing service operated by the McDonald-Douglas Corporation. Information is extracted from the admissions forms and entered into this system via computer terminals in the business office of each hospital. The information is processed in Peoria, Illinois, and bills for insurers and patients are printed out at the hospital. In addition, daily census reports are prepared for each ward and a variety of statistical reports are produced for administrative purposes.

As it now stands, the billing system contains information on each patient's age, sex, race, family background, ward and source of payment—in addition to basic identifying information. In the future, according to Medical Records Director Bliss, the system will also contain information on diagnoses and medical procedures—the full range of medical information required for reporting to insurers and government agencies.

The unpaid bills of patients are turned over by the Center to the County Bureau of Resources and Collections, whose functions include collecting delinquent hospital bills for the entire hospital system. The Bureau pressures the patients to pay, and where this doesn't succeed, they refer the matter to the County Counsel's office, which can take the patient to court, attach personal property, or place a lien on the patient's house or land. Because this is time-consuming, it is done on a selective basis, primarily to give credibility to the enforcement process.

Medical Records and Admissions workers estimate that about 5% of patients give false names and/or addresses, and only occasionally will such false identities be uncovered. Some patients do this because they are afraid of the hospital bills, others fear deportation as illegal aliens, and still others do not want to be stigmatized by an illegitimate birth or venereal disease.

Despite current collection efforts, reimbursement for County medical services remains a chronic problem. In July of 1974, the Audit Committee of the County Grand Jury handed down a report criticizing the Bureau of Resources and Collections. The report noted at least $2 million outstanding in delinquent hospital bills, and singled out Medical Center's Emergency Room billings as being in particular need of improvement. The report called for more effective collection procedures to be established, such as billing emergency room patients at the time of treatment and more quickly identifying those eligible for MediCal.

It should be noted that the Medical Center must accept any acutely-ill patient, regardless of financial condition. The Center has tried to delay treatment in non-emergency cases until it found out who was going to pay for it. "This was abandoned," said John McClurg, the Center's Medical Service Administrator, "because the additional revenues we got by this method didn't balance against making the patient wait longer."

In addition to its payment function, the admitting form also serves medical purposes, and these have been enhanced by computerization. For example, the Center has special information on 8,000 Medi-Alert patients which can be printed out on the application record; this warns the staff about these patient's special medical problems. If a patient is a diabetic, for instance, a code number appears on the Application Form that places the patient in a special ward. Or if a patient has a pacemaker, a phone number will be provided for special instructions.

The Patient's Medical Record Within the Hospital

When the admission procedure is completed, copies of the application record are sent to the Department of Medical Records, the Chaplain's Office, the Data Processing division, and Patient Billing. It is also attached to the patient's chart - a collection of laboratory reports, X-Ray results, diagnoses, etc. - which is compiled for immediate use while the patient is at the hospital. These individual patient records are kept manually.

A physician may call for a previous patient record stored in the record center to be produced for use in this treatment episode. This is not done automatically, however. According to Andrew Bliss, Director of Medical Records, physicians request a search for prior records on only a third of their patients. There are several reasons given for this limited use of past records:

1) They are not always delivered as fast as the physicians need them, although Medical Records Director Bliss states that they are usually delivered "within thirty minutes after a request is made."

2) The needed information must be laboriously extracted from the collection of paper forms, notes and X-rays that make up the patient's permanent medical record. "Right now, we have no economical way to do this," reports Professional Services Director Sol Bernstein. A survey by the Chief Registrar of the Center indicated that even when the past record is requested, physicians on the ward look at only 5% of the items on the chart.

3) Identification problems sometimes result in the wrong record being delivered or information on more than one patient being included in the same record.

4) Physicians often will not accept the "work-up" done on a patient prior to the current admission. Dr. Bernstein points out that "A physician here will order a new work-up even if the person was recently a patient in his own hospital. It's a combination of careful medicine and mistrust of the other man's work."

Some of these difficulties are reflected in the findings of outside review bodies. In 1972, the Joint Commission on Hospital Accreditation withheld the Medical Center's normal 2-year accreditation. The decision was based in part on record-keeping shortcomings, including failure by physicians to sign requests in patients' files for treatment and X-rays, failure to complete discharge summaries and operation reports on time, and failure to establish a sufficient number of audit committees for internal review of the staff's work. A year later, however, the Commission found many of the record-keeping deficiencies corrected. The State Department of Health, in reviewing the Medical Center, has also commented on improperly signed orders for treatment and failures to identify patients accurately.

Whether the chart is a new one, or one continued from a previous stay, this chart follows the patient. If the patient is admitted to a ward, the chart is delivered there, and is stored on a rack outside the nursing station. If the patient moves to another ward, the chart follows along. "We're talking about an enormous demand here ...moving hundreds of large records around every day," comments Mr. Bliss.

The Growth of Computer Use at the Medical Center

Why did Los Angeles County move into electronic data processing? In the late 1950's, the Medical Center began to convert its payroll and patient billing from manual to machine processing. "As the workload grew," said Gene Thompson, Chief of the Health Information System, "they just kept developing along proven lines, adding more of the same kind of equipment until they had a big tab shop with perhaps 75 people."

In 1968, following acceptance of the computer studies mentioned earlier, the Medical Center acquired an IBM 360/40 and began converting its admissions system. By the end of the year, on-line records for 65,000 patients were available at the Medical Center via twelve terminals. Developing this system did not involve converting much of the data from existing manual files but was designed to build its own data base over time. Use of the system created the list of past admissions against which current patient identifiers are checked.

In 1969, the Data Processing Department began to expand the system beyond the Medical Center complex to all nine county hospitals, and to the present 120 terminals and almost two million patient names. The MedicAlert previously mentioned was created. A variety of administrative and statistical reports are also generated from data already in the system or especially in-put for processing.

In addition to the functions of the main computer, several stand-alone computer systems developed independently. Among the separate systems are: (1) processing and reporting blood gas analyses and electrocardiograms; (2) keeping track of X-rays; (3) patient-monitoring at Women's Hospital; (4) scheduling clinic appointments; (5) keeping track of the hospital's 2,000 non-resident attending physicians; (6) keeping track of prescriptions and drug use in the pharmacy; (7) monitoring vital signs in the cardiac intensive care unit; (8) statistical and administrative information about patients with communicable diseases and mental health problems.

According to the Health Information System's chief, Gene Thompson, most of these systems developed out of very specific needs and were "shepherded by one or two people who could make a case for getting the money. Almost all of them were developed in-house in an ad-hoc fashion. They're not part of some grand design."

Lack of research and development money seems to be the chief reason for this ad-hoc development of computerization. Mr. Thompson recalls that "...we had to develop applications that showed pay-off because most of the money for development came out of the County. Even though the environment in the County was pretty encouraging for EDP -- Medicare and MediCal dollars had just started flowing in --- we had to develop very practical applications. We knew from the beginning that we were going to develop a system that would grow slowly and that would change over time. This kept us from even thinking about putting it all together in one big 'hospital information system.'"

Both McClurg and Thompson point to a second constraint, in addition to the lack of money, - the early focus on serving multiple hospitals made them reject the idea of building a system to handle all the records on all patients. "There was just too much there; it was clearly too complex to do all at once," said Thompson. "So we thought in terms of being able to do the job both manually and on the computer. We vowed never to try and replace the whole chart."

Hospital personnel interviewed believe that the computers save time, improve record-keeping accuracy, and provide better administrative handling of patients and their records. As to the Admissions/Identification system, Thompson states that "The average admission time has been cut from 15 minutes to five or six...In addition, admissions forms which go into the patient's chart are more standardized and have fewer errors than in the past." Computerization has also enabled County hospitals to achieve some limited cross-referencing of patient files. One of the early problems encountered was that a clerk in one hospital was able to introduce errors into the files of another hospital. When this kind of error reached intolerable levels, the system was changed so that a terminal user in Hospital A could read but could not add to or alter the identification files of Hospital B.

Since the Admissions/Identification system links separate medical records, but does not create a consolidated record from several sources, its operation has had little effect on the accuracy of those medical records which still depend upon manual entries. A review of the Medical Center computer system found that: "Level of efficiency in linkage was considered good, but only as good as the actions of people who back up the system and the quality of the service given as a result. Quick and accurate reference to the medical record...was considered futile if the record was not completed accurately, not filed currently in an accessible manner, and not deliverable within a minimal time lapse."

Two important medical applications currently being developed are a laboratory data management system and an expanded pharmacy system. The laboratory system, under development for the past six years, includes both analogue and digital processing. The labs at the Medical Center are now fully automated and hospital officials describe them as the largest clinical testing complex in the country. Over, 1,400 kinds of tests are performed, for a total of 7½ million procedures each year. The diversity and volume have proven difficult to handle, but Thompson expected that a system to print out lab results summaries on demand in the admitting and emergency areas, and report these to the patient's chart would be ready by the end of 1975. At first, this system will serve only the Medical Center, but will ultimately be expanded to all the acute hospitals.

The goal of the pharmacy system is to focus the physician's attention on over-use of particular drugs, bad drug combinations, and patient sensitivity to medications. "Basically, the system will tell the physician what the preferred drug is for the diagnosis. It will also keep the patient's drug history file up to date and check to see if the patient has ever had a reaction to the drug prescribed."

Citizen Rights Issues

We noted earlier two basic aspects of the Los Angeles systems that frame its treatment of citizen rights issues. First, most are poor, members of racial minority groups (primarily black and Chicano), likely to be dependent on welfare and other county social services, and often of low or little literacy. Second, the hospital system is understaffed and over-worked, and its patients' medical problems are often the result of urban poverty and social neglect over which patients and hospital staff alike are powerless. The situation resembles closely what the documentary filmmaker Fred Wiseman found when he did a film on Metropolitan Hospital in New York City. Wiseman* went expecting "to find a lot of bureaucratic callousness and a hardened staff, indifferent to the problems of the poor. What I generally found, though, were a lot of doctors, nurses, and hospital personnel who really cared" but were basically unable to overcome the "medical consequences of bad housing, illiteracy, no jobs, malnutrition, and so on." When issues of rights such as privacy, confidentiality, and patient access to records arise, the problems are further compounded because many hospital officials regard these as "frills" and "expendable" matters, and many patients in a place like Los Angeles Medical Center simply do not know that they have any rights at all.

Confidentiality

As in other hospitals, Medical Center personnel begin with the conviction that a patient's medical data is"confidential." But exceptions to this rule come in legions. When the patient is admitted, except in emergency cases where the patient is unable to do so, all patients or their legal guardians must sign a General Consent form before treatment begins. The patient "agrees to" whatever tests and medical procedures the hospital staff deems necessary, including discharge to another public medical institution. Since this is a teaching facility, the form also specifies the patient's consent to "demonstration and/or observation" by physicians, medical students and student nurses. Finally, the patient also formally consents to "...release of medical information to other institutions or agencies accepting the patient for medical or institutional care; (and to) patient's insurer." A copy of this form, which is in English and Spanish, is given to the patient, and the original is attached to the patient's chart.

We have already noted some of the ways in which outside non-medical personnel obtain access to patient information at Los Angeles Medical Center, such as the joint Commission on Hospital Accreditation, which conducts chart review for accreditation purposes, or the State Department of Health, which also conducts chart review as part of its yearly inspection routine. Among other outside non-medical agencies or individuals who share patient information are the following:

1. Insurance, Medicare, MediCal. Each month, approximately 4,000 reports go to private insurers, and to California Blue Cross which acts as intermediary for Medicare and MediCal. The claims form includes a brief "discharge summary" - dates of admission and discharge, diagnoses, a history of the problem and a list of surgical procedures. Similar information, in somewhat greater detail goes to Blue Cross for its own use.

---

*"You Start Off With A Bromide: Conversation with Frederick Wiseman," The Civil Liberties Review, Winter/Spring, 1974, Vol. 1, No. 2, 57.

The claims forms are prepared from the patient's record, drawing on the physician's formal discharge summary. Where no discharge summary has been prepared (the large backlog is a chronic problem) a summary is constructed from recent materials in the record. The general consent form that the patient signs upon admission covers the release of this material. In addition, most patients sign a release as a condition of receiving state or federal aid or private insurance.

2. Employment, security, life insurance, disability, investigations. The Medical Records Department responds to about 18,000 ad hoc requests a year for information from patient records. The inquirer generally has an authorization form signed by the patient as part of his application for insurance, filing a disability claim, employment application, etc. An average of about one request a month is turned down, generally because the inquirer did not have the proper authorization.

A records department worker describes her job this way: "They come in and we make them sign the log we keep of all the people who look at records. Then we're supposed to check the patient authorization form. If it is more than six months old, we refuse the request. When we locate the record, we check the signature on the form against the patient's signature in the record. Then we either type out a summary for them or let them sit down with the record." The hospital will copy a record only if it has been subpoenaed, but lawyers and insurance company representatives often bring their own copying equipment to the Medical Records office, and are generally allowed to use it.

Routine claims-information requests concerning psychiatric treatment are handled like other medical treatment requests. But requests from lawyers, or from insurance or employment investigators, require the Assistant Director of Psychiatry to authorize the release if it seeks anything more than dates of admission.

"Most of the requests we turn down are in the mental health area," says Medical Record Director Bliss. "Let's say a man applies for a job and he was treated here five years ago in the psychiatric service. The Assistant Director might refuse to release a discharge summary if he feels the person's problem is not relevant to the job applied for. The job applicant may have signed a release, but the law allows the psychiatrist to refuse the information if he thinks it is in the best interests of the patient to do so."

This may create a dilemma: "Sometimes we get a security investigation case," says Mental Health Services Head Clyde Johnson, "where we stand to hurt the patient if we release the information on file — because it might be misunderstood. The investigator can assume that since the patient has signed a release, but we have refused to give it, the information must be really bad."

3. Public Reporting Requirements: Physicians are required under California law to report injuries they think were the result of a criminal act, either self-inflicted or from violence by another person. Assistance Medical Records Director Faulkner states that "Where it is the physician (rather than the police) who discovers a knife wound, say, or a battered child, he just notifies Security and they notify the Los Angeles Police."

Communicable diseases, such as V.D., and drug overdose cases, must be reported to the Department of Health on standardized forms. In the case of V.D., although the

Health Department follows elaborate procedures for protecting the confidentiality of those on whom they follow up, there is widespread resentment by Los Angeles County patients against the mandatory reporting, since it is widely believed that the private physicians who treat the more affluent protect their patients by ignoring the reporting provisions of the law.

4. Law Enforcement: FBI and Immigration investigators occasionally check medical records. Records workers report that: "They show their identification and sign the log. Usually they are just checking out someone's story. They want to know the dates we treated the person, what the ailment was, that sort of thing."

For the last four years, the Los Angeles Police Department has had a liaison officer working in the hospital records office. "Before this time," Bliss recalls, "all divisions of LAPD were coming in here from everywhere and it got pretty hard to keep track of. So when LAPD suggested filtering all requests through an officer permanently stationed here, it solved a lot of problems. The officer interviews patients who are victims of crime - with their permission - and interrogates prisoners in the jail ward. He handles information requests from LAPD officers, most of them over the phone." A Sergeant on duty said, "Sometimes we need to locate a victim who has already been released. We can check to see what address he or she was discharged to. We also get missing persons cases...We can check the daily admissions report for a psychiatric admission, maybe. Then we call the ward to check the identification further. What additional information we get depends on ward personnel. I don't actually let anyone handle the record. Even if another officer did come in, he couldn't just sit and browse. Where mental health is involved, I can look at the record, but I couldn't use anything from it except for locating a person. Sometimes we can pull good identifying information like Social Security number or Military I.D."

Patient authorization for release of information is not required by law or by the hospital for public reporting requirements or for inspection by law enforcement officers.

5. Civil Suits: Once a patient has filed a disability suit, a malpractice suit, or a suit for damages resulting from an accident, his medical file may be open not only to his own lawyers but to the opposing party as well. When the patient's record is subpoanaed, the whole record is usually copied and sent to the clerk of the court: there it is kept "closed" until the judge determines that it is relevant to the case. It is, however, put into the file of the case, and that is open for anyone involved with the case to see.

A lawyer in the Public Defender's Office comments that "Should you need medical information to help you impeach a witness, you may be able to get good leads from the patient's physician. He may be reluctant to talk about the case, but most physicians dislike taking a day off to go to court and testify. So you can threaten to subpoena him, and he'll tell you enough to get you started."

6. Public Inquiries: Those who enquire about a patient at the hospital are given only a brief "condition report", in addition to the fact that the person is a patient at the facility. Hospital rules forbid staff members to release more information about a patient. According to Bliss, "Very few public figures come here, so we don't often have a problem of keeping reporters away." The hospital does treat patients who have been involved with the police, however, a 50-bed jail ward is part of

General Hospital. "These patients are in the custody of the Sheriff's Office," said Bliss, "so we turn enquiries over to them. At one time we had the brother of Sirhan Sirhan here. There were many inquiries about his specific condition, and he was in the psychiatric unit so the matter was even more sensitive. We just left it up to the Sheriff what he wanted to release."

After the patient leaves the Medical Center, his or her record is sent to the Medical Records Room at General Hospital, where it will be stored for approximately five years. After this time, records are sent for ten years into permanent warehouse storage in the County Archives.

Confidentiality of Patient Records Within the Hospital

The preceeding discussion described the broad dissemination of patient information that is made to outside, non-medical agencies, either without the patient's knowledge and consent, or with a pro forma consent to which the patient must agree in order to receive medical treatment. Part of this pattern stems, as previously noted, from the lack of financial resources which compels the hospital to focus on the patient's financial eligibility. Part of it stems from the perception of the patient by the staff as a passive recipient of medical treatment - a person unable to understand the treatment, unable to contribute his own reactions, uninterested in his own record, and therefore unconcerned about its confidentiality. These staff perceptions also dictate the way in which medical records are shared within the hospital.

Members of the nursing staff believe that patients are not good sources of information about their own medical problems. Sometimes there is a language barrier. But even where there isn't, the patient may have been told so little about his condition during past visits that he cannot offer reliable information. "Half the time our patients don't even know why they are here," said one nurse. "They are often very confused and upset by the whole experience. Only rarely are they concerned about what you are writing down in the records."

The practice of collecting a broad range of financial information for eligibility, the searching interviews with the Financial Service workers, and the storing of the patient's chart in an accessible place at the ward nursing station are not seen by the staff as creating patient resentment over violations of confidentiality.

Patient data in the Admissions system are available in nine hospitals via almost 120 terminals. Health Informations System Chief Gene Thompson believes that security of this material comes from the fact that "most people don't know what data is in the system...We could have sensitive psychiatric data in there and most terminal users wouldn't know how to get it out if they were asked." 3,000 cardiac histories are given extra protection by limiting their dissemination to the two terminals in the EKG unit. Thompson adds that early in the development of computer applications for County hospitals, the decision was made that control over release of information and responsibility for its protection would remain in the hands of the Medical Records Department, the same unit which controls release of the manual records described above.

Medical Records Director Bliss states that if you "really wanted data out of that (computer) system and you could convince a clerk to do it, there's nothing to stop that. There's no such thing as a perfect system."

Neither Medical Services Administrator Dr. Sol Bernstein nor his counterpart on the administrative side, John McClurg, could remember many complaints involving confidentiality of the hospital's records. Bernstein said, "I do remember one case where a person wrote in to complain. She had transsexual surgery performed and at some later time had seen a copy of her medical record. In it, she found herself described as "he" in quotation marks. She found this offensive and wanted the slurs removed."

Bernstein went on to observe: "Most of our patients are not as sophisticated as patients in private hospitals, so they don't raise complaints often. In a training institution like this—particularly a public one—the record is a very open one. We'd like it to be otherwise. Even our staff members raise the issue. A short time ago, interns and student nurses raised the issue with respect to their own medical records." Some of them receive treatment at county medical or psychiatric facilities, including the Medical Center, and they worry about who among their colleagues might gain easy, albeit unauthorized, access to the records.

Local American Civil Liberties Union chapters and political groups in Los Angeles report few complaints on confidentiality issues in medical records. Speaking generally about the problems which low income patients face in California, Kenneth Wing of the National Health Law Center at UCLA said "The right to keep your medical records confidential is an obscure legal right, almost totally unenforceable. The institution knows that the patient won't sue because of it. Also, it's a luxury issue that no legal-services agency will handle when legal resources are limited." He did report that "some cases involving confidentiality have come here. For example, one patient felt that there were inaccuracies in her psychiatric record. She couldn't get to the records, which were in a state facility. And God knows who had access to the information. She thought there was mis-diagnosis about ten years ago and it came up in some employment process. But we said, given our limited resources, we couldn't pursue this."

Patient Access

Under California law, the patient has no guaranteed right to see his or her medical record personally. However, the patient can authorize an attorney to see the record, and some hospitals have extended this to include showing patients their record whenever they say they are contemplating litigation. Los Angeles County does not do this. As to malpractice, doctors are adjured to take pains to get the necessary consent forms for surgical and other procedures (which presumably are not covered by the general consent form signed by the patient upon admission) and in getting such "informed consent" the patient must be told something about the upcoming surgery. Of course, getting informed consent here is for the protection of the doctor, not for the information of the patient.

In the normal course of a hospital stay, the patient is told little about his record. The following staff comments speak for themselves: A nursing supervisor: "Sometimes the patient wants to see the chart when they've been kept virtually incommunicado for some time. The patient may want to know how the X-rays came out because nobody told him. Or the patient may just want to know what's happening to him and what's going to be done."

The Nursing Services Administrator: "If they've had an argument with their doctor, or they've gotten upset and thrown something at a nurse, they want to see what's been written about them. They don't want to be written up as a troublemaker. Sometimes it's more of a medical matter that they want to control, like whether the doctor describes their problems as "alcohol related."

Because patients are billed at a flat daily rate, and the bills are not itemized, patients sometimes go to the Medical Records Department for an explanation. Assistant Medical Records Director Faulkner says that occasionally the Records staff will sit down with a patient and go over the things that the bill covers "if we think it will help."

The staff does not recall ever having been sued over a patient access issue, and receives very few complaints about it. Dr. Bernstein comments: "As a matter of hospital policy, the patient ought to know as much as possible about his condition. The patient moves from place to place for care, and his records don't always catch up with him. But it's hard to keep a patient informed in a public hospital setting like ours. And I'm not sure that just giving the patient his record is the answer."

Informed Consent

The issue of informed consent was raised quite sharply in 1974 when a group of Chicano and Black women sued the Medical Center, claiming that they had been sterilized without knowledgeable consent. One of the women noted that she had worn an IUD device for two years, not realizing that she had been sterilized in the course of a caesarian delivery. The women sought damages, and asked the court to force the hospital into compliance with new HEW regulations on consents for sterilization.

Under court and community pressure, the hospital has increased its efforts to comply with HEW rules. A new consent form, in Spanish as well as English, was adopted which explains the procedures and their consequences in language at the 6th grade level. In addition, a 72 hour waiting period is observed, where possible, between consent and the operation. Civil liberties lawyers who work on such problems (including the lawyers for this case) generally agree that the HEW regulations are adequate. The problem, they say, is that most hospitals operate in such a way that it is very difficult to enforce them. Bliss noted that the suit has had the effect of making the hospital staff more cautious in sterilization cases. "There's more staff consultation and we've tried to increase supervision and counselling so that no one signs a consent when they are not in a position to think about it clearly." Recently, there has been some discussion of preparing a consent form in still simpler language--perhaps at the 3rd grade level.

Observations

Los Angeles County's Medical Center shows what happens to citizen rights when computerization unfolds in a setting of medical efforts to provide acute care under ghetto conditions. The pressure to recover costs from as many people as possible is the underlying reason for demanding extensive disclosure from patients, and this forced computer efforts toward fiscal applications rather than the emphasis on patient care that the data bank project originally hoped to maintain. Providing patient dignity -- of which rights of privacy, informed consent, confidentiality, and individual access are prime components -- is a casualty to the rush of hospital personnel to handle the daily pressures -- drug overdoses, acute alcoholism, baby batterings, lead poisoning, and all the other medical stigmata of life in East Lost Angeles.

Of course, there are difficult issues here; the civil liberties values do have to be weighed against needs of law enforcement, monitoring health care eligibilities, protecting public health, etc. But at Los Angeles County Medical Center today, there is so little balance at work; no-one within the Center staff or outside groups are there to put the civil liberties values into the other scale, and call for sensitive judgments to be made.

If American society were to decide that rights of informed consent, confidentiality and patient access were to be defined and protected, making these meaningful at urban hospitals such as Los Angeles County would require both financial and personnel resources. New consent and confidentiality rules and procedures would have to be posted and explained, and their observance policed by patients' rights advocates or ombudsmen. Enlarging patient access would take a major recasting of medical-record notations into language intelligible to the lay person, a process strongly advocated by "consumer oriented" medical experts such as Dr. Lawrence Weed, who see such disclosure as a vital part of patient participation in the health-seeking process. Staff time would also have to be provided to hold conferences with Los Angeles' patients to explain the record, and to answer questions. This type of patient-hospital relationship has thus far been limited to a few elite institutions, usually with middle and upper class patients, and even fewer community health centers treating the poor.

Some progress toward such practices may well be mandated by law. A bill to create a California Fair Information Practices Act, introduced in 1974, would regulate the use and transfer of all personal data in the personal data systems of government agencies, whether state, county, or municipal. This would include medical records, and would strengthen both confidentiality rules and patient access rights in public institutions. The bill was passed in 1975 but was vetoed at the last minute by Governor Edmund Brown, Jr., in part because of the expense he said it would cost government agencies to comply. The bill was reintroduced in 1976 and has excellent chances of repassage. Five states -- Massachusetts, Arizona, Minnesota, Utah, and New Hampshire -- have already passed such acts in the past 2 years.

The effects of such new laws in urban hospitals have yet to be felt. It may be some time before regulations implementing them are issued and followed, and before patients begin to learn what rights they have and to exercise them. But the seeds of change are in such new laws, and their effects at institutions like the Los Angeles County Hospital System may well be enormous in the coming years.

SOURCES

The site visit to Los Angeles County Medical Center was made by Michael Baker, who prepared the first draft of the profile and revised that down to late 1975. A rewriting and reorganization of that draft for the Final Report was done by Alan Westin and Florence Isbell. Baker was also aided in background research by Ms. Gertrude Wilson, a Los Angeles attorney.

Three particularly useful publications about the Center and its computer uses are: "The Los Angeles County Patient Data Bank,: in Gerald A. Giebink and Leonard L. Hurst, Computer Projects in Health Care (Ann Arbor: Health Administration Press, 1975), 179-185; Ruby Okubo, "Record Linkage in two LA county Hospitals," Medical Record News, August, 1972, 42-57; and "Our Partner, the Medical Center," USC Medicine, Vol. 20, #1 and 2, 1969/70.

For personal interviews, we are grateful to: Dr. Sol Bernstein; Mr. Andrew Bliss; Mr. Harold Faulkner; Mr. John McClurg; Mr. Richard Midgley; Dr. Moeller; Mr. John Damate; Mr. Gene Thompson; and Mr. Clyde Johnson.

In addition, valuable information was obtained from the Southern California Chapter of the American Civil Liberties Union; the Medical Committee on Human Rights; the Los Angeles County Medical Society; the California Attorney General's Office; the Los Angeles Center for Law and Justice; and several local attorneys.

CHAPTER 6. MARTIN LUTHER KING JR. HEALTH CENTER

The Dr. Martin Luther King Jr. Health Center is a federally-funded, private facility providing ambulatory care in a poverty area of the South Bronx (New York City). Associated with Montefiore Hospital, it supplies comprehensive, continuous, and family-centered health care to approximately 40,000 registered patients, out of an area population of 90,000. A staff of 450 offers in-patient medical services, preventive care activities, chronic disease treatment, and a wide range of socio-medical programs.

The Center is as much a social insitution as a medical facility, and has been described by observers and residents alike as the most active, important, and community-accepted organization in the area. Patients' rights are a foremost concern — as a matter of Center philosophy, rules, training, and daily procedures. Furthermore, the adoption of computer technology at the Center has been carried out in the context of very different goals and management "styles" than in Los Angeles: a stress on the health-team rather than medical-professional model of care; major community inputs into Center priorities and decisions; and an insistence that "machines" must facilitate rather than weaken the Center's basic commitment to patient dignity and social advocacy.

Background

The formation of the King Center came from two interconnected developments in the middle 1960's: (1) the interest of the federal Office of Economic Opportunity (OEO) in funding demonstration projects for comprehensive health care in low-income neighborhoods, and (2) the desire of Dr. George Silver, Chief of Social Medicine at Montefiore Hospital, to develop an out-patient group practice for the area's overcrowded hospital clinics and emergency room facilities. Silver was also influenced by a consumer-controlled clinic in Saskatchewan, Canada, and he saw some form of local-community participation as an important ingredient in his plan.

The area in which the King Center emerged was (and still is) an urban disaster zone. A 45-block section of the South Bronx, it was once a lower middle class Jewish community. But by the 1960's, it had become a poverty area with 45% Afro-Americans, 47% Latin-Americans, and 6% whites. Its statistical characteristics represent a litany of social blight: 50% unemployment; highest arson rates in the nation; 20% of the buildings abandoned; one of the highest narcotics death rates in the city; high incidence of tuberculosis, VD, alcoholism and lead poisoning; widespread rat and vermin infestation; and substandard schools, police, sanitation, transportation, and welfare services. There are four public housing developments in the area; while their physical layout is less dismal than the surrounding blocks, local community leaders call them "a high-rise, concrete ghetto," and these residents face a serious crime problem daily.

The Center opened in 1967, funded by a $1.9 million grant from OEO given to Montefiore Hospital, as the Center's sponsoring organization. In its first year, it supplied care to 1,400 registered families. OEO's guidelines for the Center were cast in the war-on-poverty framework of that period: "a commitment to the concept of redistributing power within a community setting . . . .

....and a restoration of the citizen's significance within a community." The Center spent six years under OEO aegis, expanding its services steadily. This ended in 1973, and the Center's federal support (now about half of an annual budget slightly over $8 million) has come since then from a grant by the Bureau of Community Health Services, in the Health Services Administration of HEW. The other half of the Center's budget comes from Medicaid and other third-party payers. In 1972, the Center had over 200,000 patient visits, and its Family Health Workers made over 40,000 home visits.

The Center's concept of medical care and social advocacy rests on five approaches:

1. Reaching Out into the Community

The Center's philosophy is based on the concept of community outreach. It does not wait for a patient to come to it with particular ailments, then treat just those. Rather, its goal is to practice preventive medicine by registering families and treating them on a continuing basis, starting with a general check-up. Beyond that, it seeks to identify serious community health problems, and attack them in a unified way through individual care, research, education, and social action.

Of the 90,000 people in the Center's current geographical area, 39,000 in approximately 9,400 families are registered as patients. This was originally achieved by the stuffing of mailboxes with leaflets about the Center and attending community meetings. Because the community has a high population turnover, continuing registration campaigns are needed.

Non-registered patients do not get total team care, but they are given emergency care and occasionally specialized care. As registration of families increases, emergency room use decreases. It presently stands at about 25% of patient visits, down from between 35-40% during the Center's first year.

The hope of the Center's founders was that every individual regardless of income would be eligible for care at the Center. But in 1971, simultaneously with a reduction in the amount of the OEO grant, OEO issued a regulation requiring a means test and setting a fee schedule for those ineligible for government aid. The ruling brought an angry reaction from MLK's then Director, Dr. William Lloyd.

> "The pain to be inflicted on our patients is of far greater magnitude than the blow to the Center's goal of serving the community with comprehensive care. The retired civil servant with heart disease cannot afford good ambulatory care here or elsewhere...The children of a marginally employed worker will no longer be screened for lead poisoning...We believe that the best guarantee that a single standard of health care applies to all is to treat all, without economic distinction, in the same program."

As a result of the ruling, the Center was forced to limit registration to: 1) care of pregnant women and new mothers and babies; 2) patients eligible for Medicaid; 3) patients eligible for Medicare; and 4) shut-ins. Since 80% of the community is poor enough to be eligible for Medicaid or Medicare, this meant that about 20% of the people were - and are - cut off from registered care. In addition, the registration forms had to be changed to include questions about "income" and "welfare status" which had not been asked before.

2. Community Programs

The Center believes that pursuing good health requires both patient education and social action alongside patients where conditions in the community threaten health.

Among the Center's special programs have been:

a) Lead Poisoning Prevention. The Center tested registered children from ages 1-6 who appeared to have one or more "suspicious" lead poisoning symptoms. It pinpointed those apartment houses with peeling paint or plaster, and held meetings with parents to explain the dangers and suggest prevention, and put families in touch with New York's Emergency Repair Services.

b) Drug Abuse and Alcoholism. The Center identifies addicts through check-ups and through home visits by the family health workers. They are referred to various city drug programs and hospitals for detoxification. In addition, the Center set up a store-front, walk-in center where residents may get educational materials on drugs, referrals and counselling. A similar project in cooperation with community groups was undertaken for alcoholics.

c) School Health Education Projects. Four teams of three staff members conducted 45-minute daily health sessions with the 15 eighth grade classes of Intermediate School #148. The sessions covered sex education, menstruation, human growth, nutrition, venereal disease, dental care, narcotics, alcoholism, family relations and any other questions on the students' minds.

d) Environment. "Providing comprehensive medical care to some 39,000 people living in a low income area of the South Bronx...is simply a half measure since local environmental conditions are the source of many of the area's medical problems." This reasoning led the Center into active participation with other groups to improve housing and environment through seeking housing planning grants from the federal government; negotiating with landlords for building maintenance, trash removal and rat control; negotiating with city officials to insure housing law enforcement; and finding private and public sponsors for new housing.

e) Recreation. The Center has sponsored a youth club as an alternative to street gangs; this gave instruction and help in community projects, black and Puerto Rican culture, arts and crafts, health education, and career development. It sponsored a summer recreation program in which 125 teen-agers participated.

These community programs, and the training programs, have had to be cut back or eliminated because of cuts in federal funding in the 1971-76 period, but the Center continues to pursue them as vigorously as funds allow.

3. Recruitment of Staff from the Community, and of "Committed" Medical Personnel

To recruit its general staff, the Center stuffed local mailboxes with fliers urging applications from residents and held more than 150 meetings with community organizations in churches, schools and apartment houses to explain the Center and urge people to work there. The majority of the 450-member staff, as a result, resides in the community and is 90% black or Puerto Rican, closely approaching the community's composition, now 62% black and 36% Puerto Rican.

The recruitment of doctors to reflect the community's racial composition has not been as successful. Of the Center's 98 full and part-time doctors, only 9 are black or Puerto Rican in spite of the Center's vigorous attempts to enlist them; however, many other foreign nationals serve on the medical staff; these include Indians, Pakestanis, and other non-whites. The turnover of doctors has been high, with an average service of three years or less. The original vision of the Center's founders was a cadre of permanent doctors dedicated to the family-oriented, team practice of medicine, who would provide continuity and confidence to the patients. That goal seemed practical during the 1960's when many students chose public service over professional advancement — teachers choosing ghetto schools, lawyers spurning corporate practice for pro bono firms, doctors regarding assignment to ghetto health care as an opportunity, not as consignment to "Siberia." Today, though, the Center has a predominantly short-term, white medical staff.

4. Special Training in Center Philosophy and Techniques

The Center conducts training for its staff to insure promotion from within wherever possible. At present, 26 of its 29 supervisors are community residents, many of whom were previously unemployed and inexperienced; five of its eight senior managers are community residents. Perhaps the most remarkable success story is that of Ms. Deloris Smith. Although she had no professional training, Ms. Smith had long been a leader in community affairs --in the PTA, in organizing a Credit Union, as an officer of the Tenants' Association. She enlisted as a Family Health Worker trainee at one of the Center's community recruitment meetings in 1967 because "it was November...and they were paying $55 a week to trainees so I figured that by the time Christmas came around I would have $250 saved and I could use the money to buy presents for my seven kids." Ms. Smith rose to become Deputy Director and is now Director of the Center, the first non-M.D. to hold that post.

During its first five years, the Center also conducted training for community residents so that they could get jobs elsewhere. Its training program now is much smaller than it was in 1967-1972, during which time it turned out some 400 medical assistants, technicians, family health workers, and medical clerical workers. The shrinking job market and the cut in the Center's budget have forced it to confine its training to those special Center projects where specific job skills are required.

5. The Community Advisory Board

As with most OEO programs, one of the requirements for the Center was the creation of a Board that would represent the community. This was also the goal of the Center's founders --to have a Board not of wealthy or socially prominant patrons but of people from the same social class as the patients. The Center's Board is elected by 21 delegates, who become delegates by collecting 25 supporting signatures on a neighborhood petition. The 21 delegates elect the 21 members of the Board, and are themselves eligible to run for the Board. Thus the delegates and/or Board members, while fulfilling the community-resident requirements, represent an electorate of less than 600 individuals in a population of approximately 60,000 voting age adults.

It is difficult to assess the part actually played by the Community Advisory Board in setting Center policies or in providing a community link, partly because there is not a common understanding of the Board's role. The Center's staff and the union representing the staff have feared Board intervention into management decisions, and there have been some confrontations over hiring and firing. The Community Board, on its side, has objected to being by-passed in the establishment of community programs.

Under the original OEO-Center agreement, the Community Board was meant to be the recipient of the federal grant by 1973, replacing the sponsoring Montefiore Hospital. When HEW replaced OEO as the grantor in 1973, the transfer of the grant to the Community Board was delayed indefinitely, and for this the Community Board blames not only OEO and HEW, but the Center's administration.

In spite of a history of conflict, the Center and the Board have found a basic modus vivendi. One can infer that the Center regards the Board as an important community link, although not the only one. The Board, although frustrated in its desire to get the grant funds and set policy, recognizes that the administration, as a Board spokesman said, is trying to deliver "the best services possible in the Health Center."

Health Care At The Martin Luther King Center

The community ties developed by the Center serve to break down the "we-they" attitudes that have in the past characterized many programs for the poor. When staff, hired from the community, work with community residents to secure better housing, for instance, a spirit of partnership instead of paternalism is fostered. That same spirit of partnership permeates the Center's practice of medicine.

1. Team Practice

Each registered family is assigned to one of eight health care teams. A typical health care team consists of six family health workers, two public health nurses, one pediatrician, two internists, one dentist and one secretary. A pharmacist serves two to three health teams.

The family health worker (both men and women serve in these posts) provides the closest link to the patients. After six months' training, these workers are able to keep records, perform certain medical duties, make referrals to other agencies, explain the Center's operations, assist with appointments, and generally help with the family's medical and social problems. Each family health worker serves about 225 families and tries to visit each one at least once every three months as well as to register eligible new families as they move into the neighborhood.

A family health worker describes some of the things she does as follows:

> "Mrs. A. has trouble seeing and counts on me to help get her to the health center for appointments. On the way home, I usually do some shopping for her...Mrs. B. uses a walker and I am arranging for her to get a wheel chair so she can get around better...I helped make arrangements for Mrs. D's child to get into the hospital since Mrs. D.'s English isn't too good...Mrs. E. says her 80 year old mother needs privacy and asked if I can help get an apartment with one more room. A teen-age girl wants an appointment to discuss birth control. She wants me to explain what the nurse will do and set up the appointment.
>
> "The internist asks me to check the blood pressure of a hypertensive patient... The pediatrician asks me to evaluate the possibility of child neglect. One of the children had been burned twice by hot liquid...The nurse asks me to bring penicillin to a patient who has no phone."

The Center feels that the family health worker provides the needed sense of continuity for the families under her care, and helps ameliorate the high turnover of doctors.

The team's nurses are each responsible for 650-750 patients covered by three family health workers. They instruct and assist the family health worker in medication and medical procedures, and after briefing by the doctors, care for many of the patients on follow-up visits. They are responsible for medical chart supervision. "During one recent day," reports a team nurse, "I interacted with family health workers 18 times...I communicate with the team physicians several times throughout the day."

Direct patient care at the Center takes up the major portion of the day for the team physician, who is responsible for about 2,400 patients. A team pediatrician reports:

"I have eight clinical sessions per week. I see an average of seven to eight patients per session. In a set-up like this Center, one realizes that one's responsibility to the patient does not end with just looking after the medical problem... I spend some of my time writing letters for better housing facilities and more financial assistance; contacting the Bureau of Child Welfare in cases of neglected children; talking with school guidance counselors; teaching mothers preventive as well as acute medical care...These problems are not solved overnight, but I get a good feeling of satisfaction whenever we are able to help even just one or merely scratch the surface of another."

In addition to informal conferences throughout the day, the team schedules a regular session at which all members meet for one hour a week.

The testimony from many team members -- perhaps "testimonials" would be more apt -- show their strong commitment to team practice. But the smooth functioning of the teams evolved slowly. In the beginning, family health workers resented their being regarded by nurses and doctors as mere "messengers." Doctors complained that nurses were "subservient" and avoided decision-making. Nurses, on the other hand, resented traditionally-trained doctors whose attitude was "I am the physician and I make the decisions." Doctors were criticized for "talking too much," and trying to dominate team meetings. It took years of conscious effort by all team members to get the teams to mesh smoothly and to emerge as tight-knit "family" groups. The extent to which that transformation has taken place is seen in the comments of a team internist:

"No one on the team is alone with problems of any one patient and the sharing is comforting...After learning to eat chitlins with sangria, doing the Puerto Rican bolero with my white Ozark savoir-faire and ushering at the wedding of a family health worker's daughter...being a member on an MLK team begins moving from the pages of a treatise on social psychology to a vital, rewarding experience --and I find myself in a position that I really like."

2. Medical Record Keeping

Registration at the Center is by family. A Family Registration form collects family and household identification information (names, address, telephone number, weekly incomes of family members, insurance data, e.g. Medicaid number). Each record is assigned a five-digit family identification number, and each member is then given a two-digit prefix number, e.g. head of household. This is an internal record-keeping device; the Social Security number is not used as a patient identifier as it is in some health care institutions.

Each patient within the family is then given his or her own individual record which contains the results of regular check-ups: x-ray reports, laboratory summary sheet, ECG results, as well as a continuing record of any additional medical care. It also contains a No-Show record, which we will discuss shortly.

Since 1970, the Center has been using the problem-oriented record (POR) developed by Dr. Lawrence Weed, who visited the Center in 1968 to explain his concepts to the staff. Instead of filing items chronologically in a medical record, with summeries written whenever a fresh complaint is met, the POR technique is based on development of a "patient profile" that includes both social history and medical treatments; a problem list that identifies the chief current problems and serves as an "issue-oriented" table of contents to the full record; an initial plan of management for each item on the problem list; and progress notes geared specifically to each item listed. The Center started using the Weed system in 1970 with training sessions in its proper use; between a third and a half of the charts are now kept in that form.

Computer Development

In its first few years, the Center did billings, payroll, and basic reports on a small computer, using batch-processing. Several important research studies of community health needs and patient utilization of the Center were conducted through the aid of computer data analysis, as well as a statistical audit of service delivery by professionals and staff teams, made possible by disposition sheets produced by computer.

In 1971, the Center moved to an on-line computer system. The picture of record keeping in the Center's Report for that year graphically explains why the administration felt a need to turn more heavily to computers. It described proliferating paper for which there was no room; delayed or missing lab reports; duplicate appointments and mistaken appointments causing "at least half of the no-shows;" incorrect billing; unfiled records and laboratory reports; and government reports not forwarded by the required dates.

With its 1971 expansion, the Center not only worked on those problems but also developed a monthly "profile" on each patient who had a medical transaction the previous month. This profile was attached to the patient's folder and was designed for both administrative and direct-care purposes. It served to update billings, flag routine treatments due, print out a problem-oriented table of contents to facilitate chart review, reduce duplicate appointments, remind physicians about drug sensitivities, and "identify and focus attention upon 'overutilizers' and 'underutilizers.'"

The computer was also used in 1971 to process the results of a door-to-door survey conducted by Center personnel to validate and update patient registrations, collect data to justify insurance payments for registered patients, and assign a priority based on medical need for the processing of new, unregistered residents.

The Center also expanded during 1971 its "management information system," (MIS) designed to provide the "timely and accurate" data "to formulate decisions governing operations of the Health Center, such as staffing, scheduling, etc." This MIS work was based on a set of weekly computer-generated tables reporting various activities (such as patient encounters) during the previous week. The tables allowed management to moniter individual and unit performance, and made possible better projections of monthly and annual patient volumes.

Computer development continued actively during 1972 and the Center installed a larger, IBM 360 system in early 1973. Today, it has major application systems for registrations, appointments, laboratory tests, billing, patient encounters, payroll and personnel, quarterly reports, and integrated management information. Several of these are worth noting for our profile, since they show how patient-care operations are affected by computer use.

1. Appointments

"Appointment Central," a section of the health services department, generates a master schedule of all appointments and produces a weekly appointment sheet for each practitioner seven weeks in advance of scheduled dates. Appointment sheets from each health-care unit are collected two days prior to the session and are checked against a preliminary printout furnished by the computer and last minute appointments, such as special follow-ups, are added. The sheets are sent to each health-care unit at the beginning of the month in which the appointment is made, and the receptionist mails a notice to the patient.

"Appointment Central" plans to install as soon as possible an on-line appointment system listing all scheduled appointments for a patient (thereby avoiding duplicate appointments with a single practitioner and simultaneous appointments with two different practitioners) and also displaying on a terminal screen the available appointments for a practitioner at any given session.

2. Laboratory System

The "Lab Central" application has automated much of what used to be manual laboratory clerical work. Test results are first verified in the lab as having been completed and are then sent to "Lab Central," where they are coded and processed in the keypunch and data processing divisions. "Stat" work is done and reported immediately, and physicians can now secure reports such as chemistries, urinalysis, and wet preps within a 24-hour period, where these once took 2-3 days. Comparisons between ordered and completed lab work are still done substantially by hand, but a new system being installed will permit recording the receipt of a lab result, even if the actual report must be forwarded physically to the medical records department for filing.

3. Billing System

The billing system takes encounter data, compares it against the master roster and produces a billing history file used to generate Medicaid and Medicare bills. Although the billing system has been sufficiently developed to bill Medicare and Medicaid with reasonable accuracy, the Center still has problems with inaccurate billing on the master file and missing billing information relating to patients eligible for Medicare, and it is continuing to work on those problems. Manual follow-up after treatment is still used to record the treatment, diagnosis, and name of the attending physician, since it is often difficult to obtain all of this at the time of treatment, when the patient encounter form is completed.

4. Reporting

The Center is required to submit statistical utilization reports at quarterly intervals to the Department of Health, Education and Welfare, basically to "justify (the Center's) existence to the people in Washington." The computer makes it possible to supply the data that HEW requires, such as the number of patients registered and receiving care within a given time period; the number of visits to each unit of the Center during that period; and the number of patients registered per physician or health care team.

5. Research

The Center's administration has used its "data base of medical, demographic, and management information" to support a variety of research projects in recent years. Most have been geared to improvement of the Center's medical and social programs. For example, as part of the lead-poisoning campaign described earlier, reports of lead-poisoning cases were fed into a computer file of buildings and registered children to generate reports about children in danger of becoming poisoned who had not yet been contacted or treated. Other studies have involved productivity analysis and patient flows in the pediatrics department, as well as the incidence of various specific diseases and conditions.

Overall, Center Director Deloris Smith believes that the computer has been a good tool. She says it has reduced the number of personnel needed in the medical records and billings departments; "beefed up" financial analysis and reporting; and provided the central administration with "useful information rather than a lot of useless print-out."

Even more significantly, though the top administrators and the data processing staffs are thoroughly aware of the specific computer systems, the nurses, family health workers, and practitioners whom our project interviewed were not particularly aware of what patient data were stored in the computer or how the various application systems worked. They simply took the computer-assisted operations for granted, and had learned what they needed to, in order to use the EDP equipment. They felt no conflict between their missions and the on-going computer development.

This underscores a point made in the Center's *Fourth Annual Report* (1971) by its then Director, Dr. Harold Wise. Once organizations move to "complicated technology," Dr. Wise noted, even in supposedly "consumer-controlled" organizations, "the real control" usually "is taken over by the managers...the layman must depend on the expertise of those who work with technology to make the decision." This was especially true in the health area, he noted, where the technology "is complicated, magical and mysterious, and the quality of service difficult to monitor." One does not feel this from observing the daily routine or talking to staff at Martin Luther King. There is no sense of roles having been reorganized around "computer needs" but, rather, of the basic health-team approach and staff social-advocacy activities having been intelligently supported by EDP capabilities. No-one visiting the Center would imagine that the systems analysts, rather than Deloris Smith and her colleagues, are in charge here.

Citizen Rights at the King Center

The conventional wisdom is that the poor are so beset by the problems of economic survival --unemployment, poor housing, undernourishment --that refinements like dignified treatment, including privacy, are unimportant or at least secondary considerations. This conception of economic priorities is an arguable one. To site several noted instances that run counter to this judgment, and involve Dr. King's own campaigns, we need only recall that the Montgomery, Alabama bus boycott of 1956 did not begin because the poor blacks of Montgomery were seeking lower bus fares. They were protesting the indignity of being forced to sit in the back of the bus. Similarly, while Dr. King's campaign in 1963 against segregation in Birmingham was directed partly against job discrimination, the issue that struck the deepest chord in the local black community, and became the focus of national demonstrations leading up to passage of the federal civil rights act of 1964, was also a "dignity issue" --the refusal of white merchants to serve blacks at lunch counters and other public accommodation facilities.

The Center's Health Advocate (a position created to represent and protect patients' interests) put it this way: "Traditionally, health facilities are not interested in dealing with the rights or feelings of the patients. At MLK, we feel that being sensitive to the emotional needs and desires of a patient is as much an integral part of the treatment plan as the actual prescribing of medicine."

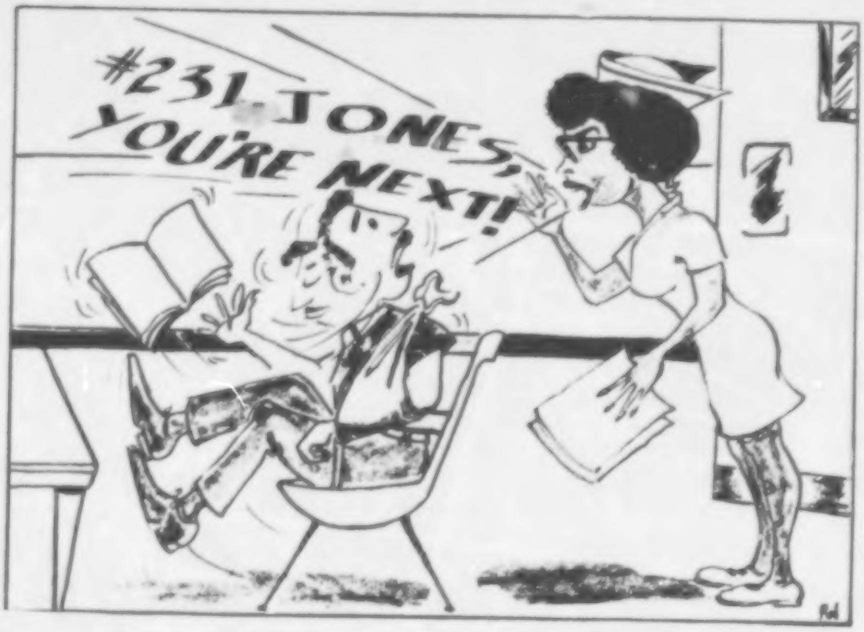
While it knew that these were its objectives, it took the Center about a year to formulate what patients' rights meant in practice, since there were no ready models to copy from other health centers, or in the health literature, or in legal procedures. A survey was conducted among patients, staff, and administration to find out "what patients' rights meant to each of them" and what should be formally declared by the Center. This led to the writing of a clear and cleverly illustrated booklet, "Your Rights as a Patient," done in both English and Spanish. At the same time, the Center adopted a formal grievance procedure for patients and made the Health Advocate a representative of the patient, who was to follow all grievances to insure their proper handling.

The rights set out in the booklet are: (1) the right to courtesy and respect, (2) the right to refuse treatment, (3) the right to a clear explanation of procedures and treatment, (4) the right to privacy, (5) the right to choose a convenient time for appointments, (6) the right to transportation to and from the Center when disabled, (7) the right to assistance in applying for Medicaid, and (8) the right to informed consent with respect to the exchange of information between the Center and other agencies (e.g., schools and referrals).

How several of these rights are explained to patients deserves reproduction here from the booklet:

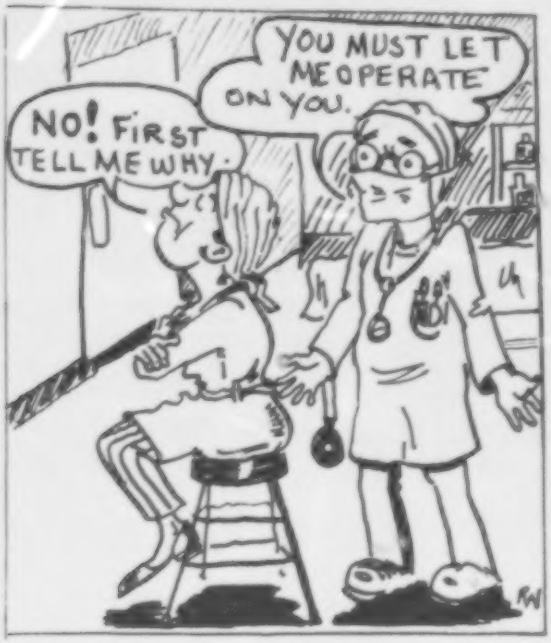
DIGNITY

You have the right to be treated with respect. You should be called Mr. Jones, not number 231, and not Jones.


#231 JONES, YOU'RE NEXT!

RIGHTS IN THE TREATMENT ROOM

a) The patient has a right to consent to, or refuse any treatment.

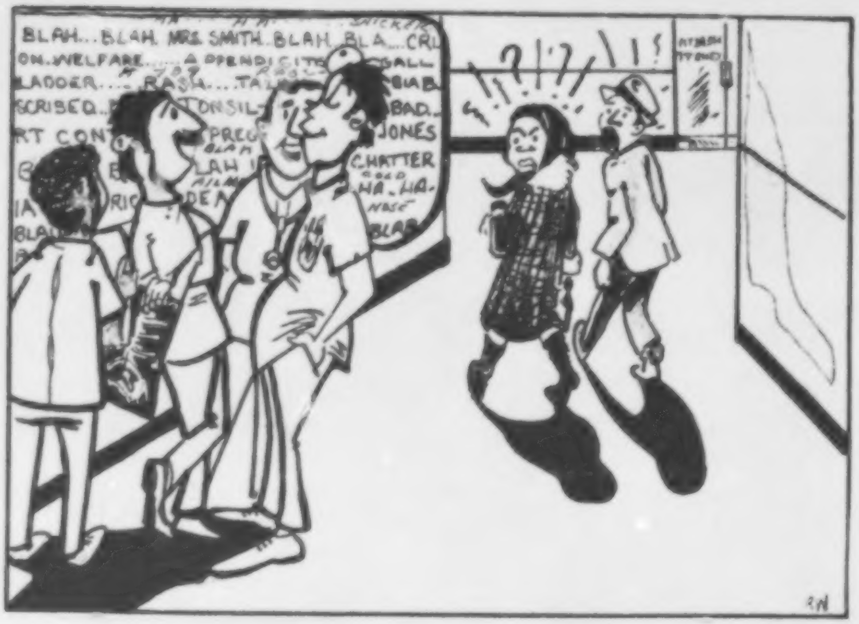

YOU MUST LET ME OPERATE ON YOU.
NO! FIRST TELL ME WHY.
RW

b) The patient has a right to have things explained clearly. (For example, any possible side effects of medicines.)

c) The patient has the right to refuse treatment by any physician and to request a different doctor.

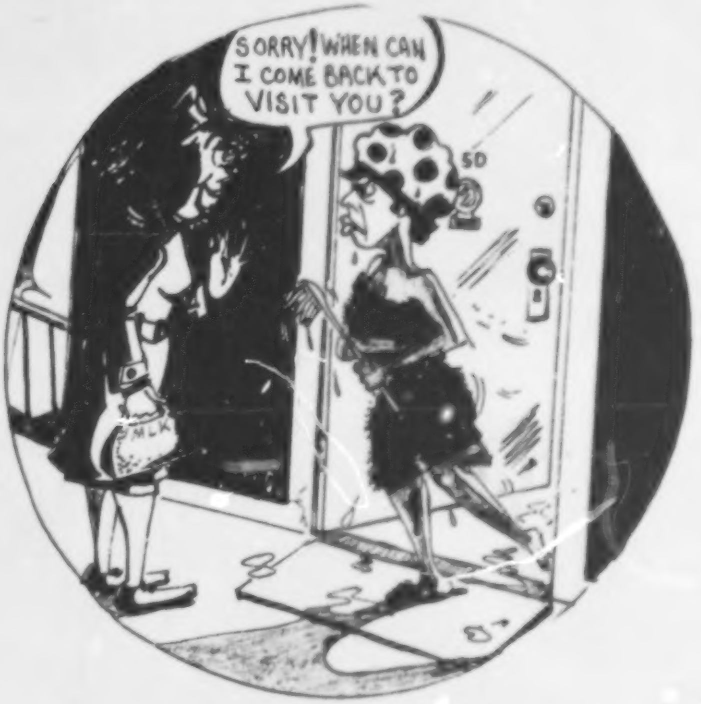
PRIVACY

a) No employee should talk to you about your problems in the waiting room or halls or where others may hear.


BLAH...BLAH. MRS. SMITH. BLAH. BLA...CRI
ON. WELFARE...... APPENDICITIS ...GALL
LADDER.... RASH.... TA
SCRIBED.. TONSIL BAD..
RT CON PREG JONES
BLAH
LAH CHATTER
GOOD
DEM HA..HA.
IA RIC NOSE
BLA BLAB
?!?!!!

b) No one should call across the room for personal information. For example, "Do you have Medicaid?" etc.

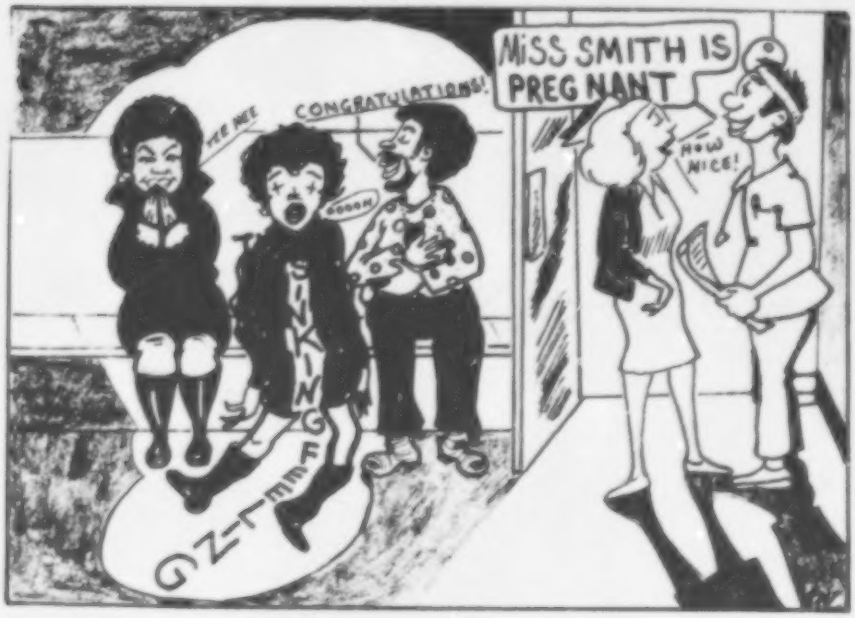
c) You have a right to consent to any visit to your home. If at all possible you should know in advance when the visit will take place.


SORRY! WHEN CAN I COME BACK TO VISIT YOU?
5D
MLK

d) You have a right to refuse to participate in or be interviewed for research purposes. You have the right to full explanation of purposes and uses of the information if you do participate.

CONFIDENTIALITY

a) The patient has a right to have all information about him held in strict confidence by Health Center staff.


TEE HEE
CONGRATULATIONS!
OOOOH
SINKING
FEELING
MISS SMITH IS PREGNANT
HOW NICE!

b) The patient has a right to see letters, know about conferences about him and results of conferences. (Patients must sign all letters.)

The booklet concludes with an explanation of the complaint procedures, and contains a complaint form which can be detached and mailed in to the Community Health Advocacy Department.

The Center's booklet, it believes, was the first such publication for patients in the country. Since then, it has been widely copied by community health centers, though not by many government hospitals or private health centers.

According to the Health Advocate, Liery Wynn, "the Patients' Rights pamphlet led to changes in the system of health care delivery." The way in which the rights it identified have been further defined and treated in practice, and how conflicts between Center positions and outside pressures have been handled, were a primary focus of our visit to the King Center, and produced the following detailed portrait.

1. Right to information

The Center's pamphlet tells patients "You have a right to know what is going on. Always ask questions about anything that you do not understand or that is worrying you." Probably the most usual mechanism for enforcing this right is the close bond between the Family Health Worker and the patients; the health workers are often not only explaining terms and procedures but also telling the doctors and nurses that the patient is uneasy or wants further explanation, and seeing that this is provided.

Two examples of such practice came in interviews with Family Health Workers that have been published by the Center. The first was with a Mrs. Montgomery:

> "I know I used to go to Morrisania Hospital before the King Center opened. And the doctor would come into the room and I knew when I told him I had a headache, he was going to give me an aspirin for that headache, and in two seconds he had gone to another patient. They really don't give you any time to question or they look at you like you are a specimen, as if to say, 'You don't talk back to me. I just tell what's going to happen to you and that's it.' And they just walk away. Sometimes even if you ask them a question, you don't get any answer. Or if you get an answer they brush it right off, and that sort of turns you off right there. And I think that is where the King Center is unique, because you can talk to most of the doctors here. If a patient has a problem speaking to a doctor, he'll come to a family health worker and tell her, 'Look, I asked him, but I didn't get the right answer.' And then we, in turn, would go back to the doctor and we would speak to the doctor and tell him. 'This patient does not understand what is happening. Will you explain it to her?' And most of the time the doctors will. I think that's one way that we are very good."

Another health worker, Mrs. Lamot, described her experiences this way:

> "One of the things that has helped us encourage patients to do this is that pamphlet that we have on patients' rights. I explain to the patients that if they go to see a doctor and they ask questions and get an answer that they are not satisfied with or if they are not being treated properly, they have the right to go to the family health worker or the person in charge of the patients' rights and complain. When we are on our home visits we counsel the patient; we tell them to just come out and talk to the doctor and don't be afraid because we constantly remind them that they have rights as patients. You know in other clinics the patients are afraid to speak up. But they are not here because we enforce the rule, and we teach them how to ask questions. They know that they can depend on family health workers which is good because I want them to know that they have rights so there is a good understanding between the patients and the Center staff.

How Mrs. Lamot does this was the subject of the following exchanges:

Interviewer:

Let's say for example, that a patient comes in with diabetes, and he has been put on a special diet and has to take certain pills. He knows that he has to do these things but he is not exactly sure why. How would you encourage him to get information about the treatment? How would you get him to speak not only to you but to ask the doctor? How would you encourage him to ask questions?

Mrs. Montgomery:

If a patient came to me and said, "I found out that I am a diabetic, and I know I have to be on a special diet and take special medication." I would explain to the patient as well as I could about his diet and medication. If he is still not fully satisfied, then I would take the patient back to the doctor. The three of us would sit down and the doctor would go over the whole routine with the patient: let him know just what he has to take. In that way I would get the same information from the doctor as the patient, so then I could reinforce the information the doctor told him.

Interviewer:

How would you actually go about getting the patient to ask the doctor the right questions so that in the future, when you are not around, he would know the right questions to ask? How do you teach the patient not to accept pills without knowing what they're really for?

Mrs. Montgomery:

I think that would really be patient education. When you go to the family you have to say to them, "Look don't accept everything that anybody gives you. Question that. You have a right to question it. Whenever you go to get medications or diets or anything feel free to ask that doctor what's happening with you." I think it's up to the doctor too. If a patient can go to a doctor knowing that he can ask him really anything very simple and the doctor answers that patient nicely, I am quite sure that when the patient really has questions he will not be afraid to ask the doctor. Patients follow directions a lot better when they understand what is behind them.

Interviewer:

Do you think that there is some set of questions that you can teach patients so that they know that when they have a meeting or an appointment with the doctor there should be certain questions they should always ask—there is certain information that they should walk out of that office knowing?

Mrs. Montgomery:

Yes. If, for example, a doctor is going to change a patient's medication or even if it's an old medication, the patient should speak to the doctor and ask him, "What's going to happen if I take this pill? Am I going to have a side effect? Am I going to break out in a slight rash? Will I have a headache?" And I think patients should be aware of the questions that they can ask.

Interviewer:

Have you gotten any specific comments from patients about family health workers and how the situation in this community has changed?

Mrs. Lamot:

I think we have been going through three stages. The first stage was kind of frightening because we were trying to feel our way in the community—trying to sell the Center and our services to the community. In the second stage we learned how to get a lot of things done and people gained confidence in us. We did many things for our patients. We helped them with many problems. We were doing so much I think we made them dependent on us. You know, we were running to welfare, to the hospital and so forth, and they looked forward to those things. Now, in the third stage, I think we have to learn to teach them how to help themselves, because that is part of our job—to teach through patient education. It is kind of hard for them to accept this because they have depended on us for so long.

Patients are told that they have a right to be informed about their records. In 1970, Dr. Harold Wise, the Director, saw a full right of access to the record as an important element on the Center's "consumer protection" goals.

> "In an effort to fully inform patients who wish to learn about their health status, the medical record should be made available to the patient. Those patients who wish should write a 'progress note' in the chart. Such a change in tradition would require considerable discussion with health workers who are trained to use words like 'mitotic' for cancer and 'lues' for syphilis, and whose usual attempts at communication confound the average patient. The idea is that health workers should spell out to patients the alternatives of any health treatment plan, encouraging the patient to make his own decision as to choice of alternatives."

Such record reviews do not seem to have developed, except as part of the use of the Weed problem-oriented record, with its discussion with the patient of his/her chief complaints, treatment plan, and progress notes.

Liery Wynn, the Health Advocate, reports that he has heard of only a few requests by patients to inspect their records. "The record would not be much use to the patient, anyway," he observed. "He probably wouldn't be able to read or understand much of the material in it." However, a patient is shown the record if he or she insists.

2. Privacy

The Center treats privacy in terms of respect for the individual's dignity — not exposing his or her medical situation to those staff members who do not need to know it, or to other residents who may be around the Center when the patient is there. This is expressed in the guide for medical assistants used at the Center, which contains instructions such as these:

> "The patient-practitioner relationship is a private one, and nothing that is said in the office is to be repeated. Another method of insuring this privacy is to respect the closed-door policy. The only way to communicate when a patient is in the office is by telephone, and this is to be used only when absolutely necessary.
>
> "When the patient is to be examined, the assistant should instruct him about dress preparation. When the patient is properly stripped and on the examination table, the medical assistant should cover his body loosely with a sheet, if necessary, to insure privacy."

However, if one uses the term privacy as we have generally done in this study — to refer to the right not to have someone collect irrelevant or highly sensitive personal data about an individual — then this simply does not arise as a consideration at the King Center. Implicit in the ideas of team medicine and comprehensive care is the ability to collect as much non-medical data about the family as possible to help treat the social problems of the patients along with their medical problems. ALL data is regarded as relevant. It will be recalled that when Dr. Lloyd objected to the setting of a means test by OEO in 1971, he did so not on grounds that it would require the patient to reveal information about his/her income, but only on the grounds that it would deny care to people who needed it.

3. Confidentiality: Within the Center

Family health workers receive four hours of instruction on patients' rights in their training programs, as well as a discussion of "Ethics and Conduct" that specifically includes "Confidentiality of records, medical information, patient information."

This is considered vital because team medicine at the Center means that information elsewhere restricted to the patient's doctor or nurse is shared with the entire team, including the non-medical family health workers. In recognition of the special problems created by this broadened dissemination of information, the Center has adopted the following rules to guard patient confidentiality:

A. Breach of confidentiality constitutes just cause for automatic dismissal. According to Health Advocate Wynn, every employee at the Center is well aware of this. In one case, an employee was dismissed for telling another about something he had read in a patient's chart.

B. The teams have adopted the rule that the confidentiality of patient information exchanged in team meetings must be respected. The family health worker, to whom much sensitive information is revealed, does not write down the substance of confidential communications on the record. Instead, he or she puts a "see me" note to the physician in the patient's file.

C. The presence of non-team members at weekly team meetings is carefully screened. Non members may attend only the part of the meeting for which they were invited, and their visits must be occasioned by team or patient need. Certain types of problems, such as marital difficulties, are not discussed in front of visitors.

D. Another way in which information about patients is shared among non-medical personnel is through the Medical Care Evaluation Committee which evaluates team care of patients (usually by family). The Committee consists of the Medical Director, senior internist, pediatrician, obstetrician, nurse, nurse supervisor, Community Health Advocate, family health worker and dentist. The Committee reviews patient charts, conducts a review of deaths, adverse reactions to drugs administered at the Center, and hospital referrals. Of these, the most sensitive is chart review, since obviously in the course of analyzing whether the medical team in question has provided adequate care, it also exposes the family's entire medical background to those not directly involved in its care.

The nurse who serves as secretary to the Committee comments: "Strict confidentiality concerning Committee meetings and actions was enforced and it was made clear that any breach of confidentiality could serve as a basis for dismissal from the Committee."

The Community Health Advocate's role on the Committee is to bring major complaints by patients to its attention for corrective action, and also to submit a consumer satisfaction form for the family whose chart is being audited. This form indicates that the family has been made aware of the services the Center offers, and comments on the quality of those services.

E. Special attention is paid to the confidentiality of information about minors. Because the Center not only treats minors but also runs special health education programs in the schools and in teen-age clinics, it learns of highly sensitive information about young people -- matters such as venereal disease, pregnancy, sex disorders, drug and alcohol abuse, homosexuality, and others. The Center sees a "troublesome" issue in deciding when to secure parental consent and when to treat the minor without such notification: For example, the Center's rules are that emancipated minors are treated under their own consent. Certain "mature minors" close to but not yet of legal age and with "sufficient understanding to know the significance of the consent and the reason therefore" will also be treated but the Center believes that "the safer practice is to require parental consent in these situations." If the parent refuses consent, a court order may be sought to authorize treatment the Center and the minor feel necessary. Venereal disease in New York may be treated in minors without parental consent. Interviews with family health workers confirm their critical role in assuring young people who come for treatment that the doctors and nurses will not tell their parents about things they wish kept confidential.

4. Confidentiality: Outside Agencies and Organizations

The Patient's Rights booklet says that no personal records are released to outside doctors, health facilities, or other agencies without the written consent of the patient. The Center must, however, comply with state laws requiring reports on patients suffering from gunshot wounds and cases of communicable diseases, and practitioners tell patients that they will have to do this when they begin treatment. Child abuse must also be reported, and -- along with child neglect reporting -- this can raise some difficult problems for the health teams to resolve. Here is one account of a health team deliberation about a child neglect report:

> "In this case, the pediatrician felt a report should be made, and the family health worker and public health nurse disagreed. Issues of fairness to the family, the possibility of death or injury to the child, and the effect of making such a report on the team's working relationship to a family were discussed. The family health workers were generally against reporting because they were not convinced that the Bureau of Child Welfare would be helpful to the family, and they wanted 'to give the parents a chance.' The physicians were for reporting because they had seen children maimed for life and also felt legally responsible for making the report.
>
> "In the course of several discussions...the team agreed on the following policy: Data leading to suspicion of child neglect must be clearly entered in the chart. The report of child neglect is not a punitive act; it may result in help being provided to a family...The parents should see and have an opportunity to discuss the written report before it is sent..."

There is a thread of feeling that runs through the Center's reports that does much to explain its practices as to disseminating patient information outside the Center. Given the recruitment of the staff from the community and the resulting identification with the patients, the Center 's personnel generally exhibit a feeling of being embattled and besieged by "outsiders"; by federal agencies cutting down the grant and imposing a means test on the patients; by city welfare agencies being unresponsive to their patients' needs; by Medicare and Medicaid not processing claims promptly; by absentee landlords not making their buildings habitable. This sense of embattlement makes the Center"unco-operative" when outside agencies demand information about patients that will probably be used to deny them rights, privileges, or opportunities. The Center bows to force majeur when it has to, and its annual reports are full of explanations about why certain patient information must be supplied to payers, welfare, etc. But even then, the Center maintains an active law department that brings test cases against such laws or regulations, as well as sponsoring or supporting state legislation to increase rights of confidentiality. There is no doubt that the Center uses its resources wherever possible to protect its clients.

Data Security and Confidentiality

The central processing unit of the Center's computer is housed in a locked room alongside the room where about a dozen staff members of the data processing division work on punched cards, print-outs, and data-input procedures. Keys to the computer facility are issued only to data processing personnel, and a system of access codes is used to control the availability of medical data so that only an employee with a need to know about a particular data file can obtain a print-out. Similar access controls will be used when the Center's terminal system is installed. These safeguards are seen by the Center's data processing manager as the right level to deal with "any realistic threats to what we have here."

Grievance Procedures at MLK

The Health Advocate estimates that his department gets about four complaints a week of which half have to do with administrative matters like scheduling and appointments. The others are "15% about employee attitude, 30% about treatment given by a specific employee, and 5% concern employees not explaining things so the patient can understand."

Three fourths of the complaints are resolved simply by a meeting between the Health Advocate and the staff member involved. If this doesn't work, the Health Advocate goes to the staff member's supervisor, who makes a decision that is reported to the patient within five days. Ten per cent of complaints are resolved this way.

If the patient is still dissatisfied, a conference between the Health Advocate and patient is held with the staff member and his representative, along with the department head, to thrash the matter out. Ten per cent of complaints are resolved at these conferences. The remaining 5% are those in which several patients have made similar complaints about an employee procedure, in which case changes are recommended to the Project Director and the Community Advisory Board.

In some circumstances, the fact that an advocate is an employee of the institution would cause serious concern about conflicts of interest. Such a complaint procedure in a police department, for example, usually (and often justifiably) raises the cry of "whitewash." Neither community groups nor the Community Advisory Board question the advocate process at the Center, however, nor did any persons that we interviewed. The definition of rights is so strong and clear, the advocate's role as the patient's representative is so firm, and the presence of community residents on the advocacy staff all seem to prevent any tendency for the advocate's office to become coopted by the "management."

Center Activity on City and State Computer Data Systems

Having made sure there is no conflict between its patients' rights rules and its EDP system, the Center has found itself embroiled during the past few years in an effort to see that this condition is not compromised by efforts to build regional computerized data systems.

In 1971, lawyers from the Center's Department of Community Health Advocacy were appointed to a confidentiality subcommittee of the New York City Mayor's Task Force for Comprehensive Health Planning. The subcommittee was formed to consider what protections for patient's rights might be needed if city hospitals and health centers were to have their patient data put into a regional computerized data system, which was then to be linked to a statewide planning data system. At first, the subcommittee worked its way through a series of key questions, such as whether the entry of identified patient information would require informed consent in advance; who would specify and control access to the data system; whether the individual patient would have access for the purposes of correcting inaccuracies; and whether physicians would be protected from liability if the patient saw -- and resented -- certain notations.

By 1973, the Center's representatives on the subcommittee "became concerned about the compromises of confidentiality inherent in such a system." They proposed a right by the individual patient "to opt out of the databank, forego the benefits of computerization -- the advances of science -- if one esteems privacy and confidentiality of one's medical records more highly."

In 1974, to put protections against "unsafe systems" into law, the subcommittee proposed a two part amendment to the New York State Public Health Code. The first part would limit access to patient records to persons directly associated with the treating institutions or to third party billers; in other cases, access to records would require patient notarization, identifying the person permitted access and limiting the time period to which access would apply. The second part of the proposal would guarantee the patient's direct access to his or her own record. The subcommittee's recommendations were under consideration during the 1975 session of the state legislature, and the Center was involved in pressing for their adoption.

Observations

The use of EDP at the King Center has not been as extensive as at Los Angeles County, or as pioneering as some of the other profiles we will be presenting, such as the Kaiser-Permanente hospitals. The Center is moving now into a terminal-based system of on-line computing, and this will probably lead it into a more advanced stage of computer usage, especially as far as patient profile data.

Where the King Center is an outstanding pioneer is in its definition and application of patients' rights, especially its provision of such normally "middle class rights" in a setting of urban blight, grinding poverty, and racial-minority patients. It has achieved this through the support of some dedicated people at Montefiore Hospital but the primary role has been played by talented community residents themselves, fostered by OEO and HEW grants that have allowed the Center to pursue medical and social programs that would have been impossible without such federal help. In a sense, the Center stands as one of the few remaining monuments to the war-on-poverty dream of community institutions.

But the Center's continuance is far from assured. This is not only because of its dependence on federal grants but also because of national economic distress, the withdrawal of trained medical personnel from ghetto practice, and the danger of hardening of the arteries in a middle-aged social institution that was an innovator in its youth.

Despite all of these potential dangers, the King Center demonstrates that both advanced technology and respect for citizen rights can coexist. The King Center model is there to be used by American society, if it wishes to.

SOURCES

The initial site visit in 1974 was made by Richard Silberberg and Jamie Broder, who did the first profile draft. Further interviews and telephone calls with King Center personnel and Montefiore Hospital staff were done until early 1976 by Helene Toiv and Alan Westin. The final draft was written by Westin, with assistance from Florence Isbell.

The primary sources of published material were the Annual Reports of the King Center, down through the last available one, the Sixth Report (1972-73). Also of great help was the Center's handbook, Training Community Health Workers, 1966-1974.

For interviews, we are grateful to Center Director Deloris Smith; Nurse Practitioner B. Lawson; Family Health Worker A. Davila; Medical Records Coordinator Eugenia Joseph; Health Advocate Liery Wynn; Administrator Kathleen Estrada; and Montefiore Hospital Public Relations Director Grace Urrows.

CHAPTER 7. KAISER-PERMANENTE MEDICAL CARE PROGRAM

The Kaiser-Permanente Medical Care Program is of interest to our study because of three features that are in contrast to the health care facilities we have treated so far:

1. Its patients are primarily unionized workers or middle class subscribers, not the urban poor. They pay for service, and have alternatives to Kaiser should they feel that care is inadequate or their "rights" are not being respected.

2. It is a pre-paid medical plan that is both medical provider and insurer. This means that, with a few exceptions, Kaiser does not provide third party payers--either private insurers or government agencies--with identified patient information.

3. It had five years of experience (from 1968 to 1973) with a highly advanced project on computerized patient records, and is now pursuing other approaches toward an ultimate hospital information system. Neither Los Angeles County nor Martin Luther King Center have yet automated the basic patient record, and this makes the trials and tribulations that Kaiser underwent an important experience to capture.

Background

Kaiser-Permanente is the offspring of the Kaiser industrial empire which flourished on the West Coast before and during World War II. In order to reduce the cost of employee health care, Kaiser set up its own system of hospitals, clinics and participating physicians. At its height, the Kaiser program met the medical needs of 100,000 employees.

When layoffs after the war caused membership in the medical plan to drop below 14,000, a decision was made to open the plan to the general public. Today, the Kaiser-Permanente program is the largest group medical plan in the country, a six-region cooperative system providing "total" medical care for 2.6 million people in California, Oregon, Washington, Hawaii, Colorado and Ohio. It has 50 clinics, 23 hospitals and laboratories, and employs 2,595 full and part-time physicians throughout the various Permanente Medical groups. Though there are differences in benefits among the various plans, most provide comprehensive coverage, ranging from examinations and innoculations to long-term hospital care. It is non-profit, under the aegis of the Kaiser Foundation Health Plan.

When the Kaiser plan was first begun and limited to its employees, it was considered a radical venture and aroused considerable hostility from some sectors of organized medicine. Its physicians were salaried, and most still are though some are now partners receiving percapita shares. This use of salaried doctors evoked from conservatives protests against "the corporate practice of medicine." Coupled with prepayment, this, raised even more fervent protest about "socialized medicine" and "destruction of the doctor-patient relationship."

Attitudes have changed in the last thirty years, and there is now broad recognition that Kaiser-Permanente provides some answers to widespread medical problems.* With a salaried staff, there is no physician incentive to encourage unnecessary (but often profitable) surgery and hospitalization. Prepayment enables Kaiser-Permanente to emphasize preventive medicine--catching health problems before they become costly in human or economic terms. Kaiser-Permanente members "spend less than half as many days in the hospital as other Americans." Prepayment also keeps Kaiser-Permanente premiums low - $600 a year for a family of three or more, well below the average payment for care in other plans and programs.

---

* See Sheila K. Johnson, "Health Maintenace: It Works," N.Y. *Times* Magazine, April 28, 1974, 34.

The Kaiser system has not been without criticism. Some subscribers complain that there are not enough physicians, causing patients to wait weeks for routine appointments. Some patients feel the doctors shunt them through their examinations too quickly and impersonally. One subscriber complained that he feels "like a cog in a machine." There are occasional complaints, but measured by the ultimate test of consumer satisfaction--renewal of membership by 2.5 million persons in a voluntary plan where there are ready and varied alternatives--the Kaiser-Permanente program obviously offers what a great many individuals and families are seeking in health care.

Computerization at Kaiser-Permanente

Kaiser-Permanente was a pioneer in "multiphasic health screening," in which yearly intensive examinations are offered to members along with a battery of tests designed to identify health problems early. Starting in 1950, the multiphasic screening was supported by card-punching and sorting equipment, in a manual record. But the resulting records were unorganized and difficult to use. Patient folders stuffed with documents such as lab results, surgical summaries, doctors' and nurses' notes, identification information, and sometimes even basic accounting data. In most cases, the physician lacked time to review the record and was forced into hurried extraction of those items critical to the patient's current problem. In addition, manual record-keeping costs were very heavy, accounting for 29% of the hospitals' operating costs.

In 1960, Kaiser Medical Methods Research began a pilot study, funded partly by the U.S. Public Health Service, to see how computerization might improve patient record keeping and data communication. Based on that study, in 1968, the National Center for Health Services Research, an HEW agency, awarded Kaiser-Permanente funds to develop "a computer-based system that will support the medical data requirements of one million health plan members, one thousand physicians, and a large corps of professional and para-medical contributors to patient care." The first step was a pilot project conducted in the San Francisco Kaiser-Permanente facilities, covering 130,000 Health Plan members.

Before going on to describe how the computerized patient records pilot program works, it is important to note that it is only one component in Kaiser's record keeping program. The other record-keeping elements are:

1. Administrative and Financial Records

As in many other medical institutions, computerization at Kaiser began in the early 1950's with accounting and billing. By 1973, there were "more than 400 programs utilizing EDP in administrative and financial areas. This includes generating group direct billings, mapping address and coverage changes and providing statistical profiles." These administrative and financial records are kept separate from patient records and stored centrally.

2. Manual Patient Records

All patient records, except those in the pilot computer program, are kept and stored manually in the offices of participating physicians and within Kaiser-Permanente health facilities. Manual records for patients in the pilot project also continue to be kept in this way, since the computerized records are in addition to, not in replacement of, the old records.

The pilot project system was designed to make the computerized record (Patient Computer Medical Record) the fundamental repository and basic source of patient medical information. Each computerized record was to be "a continuous lifetime record containing all essential present and future inpatient and outpatient data, including patient data from any facility and any location." As in the manual record, the file included Kaiser-Permanente medical record number, Social Security number*, name, birthdate, sex and blood type, plus enough identifying information on family members to permit cross-referencing. The medical data section of the record included historical information on past illnesses, observations by physicians, test results, preliminary and firm diagnoses, and reports on medical procedures ordered and/or performed. Financial and administrative patient data was stored separately, as with the manual system. The difference, then, between the manual and computerized patient records is not so much what went into them, but the greater ability to extract information from the computerized record, and to make additional research uses of the patient data base.

For example, with the computerized record, a physician in the Emergency Room could receive a report containing laboratory data, multiphasic data, and a listing of the patient's previous visits. Or, the San Francisco outpatient pharmacy could enter the date, time and drug data into each patient's computer medical record through interactive typewriter terminals, and the computer would then print medication labels. To refill prescriptions, the old prescription number and refill code would be entered and the entire label would be printed.

The Director of the Medical Methods Research Group which operated the pilot project is Dr. Morris Collen, a pioneer in computerized medical information systems. He believes strongly that "the advent of computers into the community will undoubtedly introduce a new era of improved health care delivery." In addition to the creation of computerized patient medical records, the specific objectives of the pilot project included computerization of all laboratory tests; development of better communication and reporting services, such as immediate (real-time) reporting of essential medical data via inter-active terminals in the emergency room or at the hospital or clinic nursing stations; testing of an admissions census system; testing of acquisitions of physicians and nurses reports in the pediatric service; acquisition of additional selected medical and administrative data, such as hospitalization utilization data.

---

* At one time it was believed that the Social Security number would become a required universal identifier, and it was asked for that reason. But Kaiser no longer thinks this and continues to rely on its own numbering system.

Starting in 1968, the pilot study applications were run on an IBM 360/50, but were changed in 1973 to an IBM 370/155. Telecommunication terminals were located at the computer center and at three Kaiser facilities: Oakland, Walnut Creek and San Francisco. The Walnut Creek terminals handled only multiphasic data, while the Oakland facility had nurse practitioner station and health center terminals in addition to a multiphasic one. The most advanced system, and the core of the project, was at the San Francisco Medical Center; the terminals here included admissions, emergency room, clinical laboratory, multiphasic program, pharmacies, outpatient encounter forms, and hospital system. By 1973, the outpatient system was handling a daily volume of 2,000 patient visits, 1,200 clinical laboratory specimens, and 1,500 prescriptions, in addition to 300 daily multiphasic visits. More than 400,000 subscribers had their medical data stored in the computer.

Citizen Rights in the Kaiser Project

1. Confidentiality

The Kaiser-Permanente Service Agreement contains the following statement: "Information from medical records of Members and information received by Physicians or Hospitals incident to the physician-patient or hospital-patient relationship is kept confidential, and, except for use incident to bona fide medical research and education or reasonably necessary in connection with the administration of this Agreement, is not disclosed without the consent of the member."

As noted at the outset, Kaiser is a pre-paid plan. Its subscribers do not have to file claims or claims information. And since Kaiser itself is the insurer, no outside non-medical agency shares patient information.

There are some exceptions.

Five percent of Kaiser's revenue comes from patients who receive Medicare and Medicaid, and one percent comes from MediCal recipients. Authorization is secured from these patients to send required information to the appropriate federal and state agencies.

When a patient is admitted to a Kaiser Foundation hospital, he or she signs a form which includes the statement: "The hospital is authorized to furnish from patient's record requested information or excerpts to any insurer of patient." Kaiser-Permanente also has a separate form authorizing them to furnish a designated party with "any and all medical information, history, records, diagnoses, reports or x-rays in your possession concerning the undersigned."

These two forms obviously authorize a broad range of information sharing, and patients are not told that they have any option to sign or not.

Recently an attorney who checked into a Kaiser Hospital for an abortion deleted the release-of-information part of the consent form. She said it was "coercive and anxiety-producing, potentially incriminating to patients, and from the hospital's point of view, legally unnecessary." When she explained this objection to the resident on duty, he called a "medical-legal" advisor, who told the patient that she could delete the paragraph.

James Sexton, a Kaiser administrative official, says that the most frequent demands on patient records from secondary users come from three sources: life insurance companies, attorneys, and law enforcement agencies. Insurance companies have to obtain a release from the patient and they do not generally ask for unauthorized information. The attorneys are usually representing patients in malpractice or third-party liability cases. As to law enforcement agencies, Sexton said that local police usually do not try to obtain information because they know Kaiser personnel are reluctant to give it. However, if the FBI is seeking information, Kaiser-Permanente officials "like to cooperate." They will not divulge any medical information, but they will usually answer FBI questions as to whether an individual was visiting a Kaiser facility at a particular time. These occasions are infrequent, and in each case, the facility administrator makes the decision about what information to release.

No medical information is provided to employers unless the patient specifically requests it. An employer can request a back-to-work slip from an employee's physician, but no medical data is included without the patient's signed authorization. Kaiser-Permanente will not normally include psychiatric information when releasing a record; their psychiatrists are particularly concerned that there be no leaks of confidential information.

In addition to record sharing with the above groups, Kaiser-Permanente, along with all California medical care providers, are legally required to supply government agencies with certain information. For example, all infectious, contagious or communicable diseases must be reported to a health officer; patients who suffer lapses of consciousness are reported to the State Department of Motor Vehicles; injuries inflicted with a deadly weapon go to a local law enforcement official; injuries deliberately inflicted on children under 12 go to the juvenile probation department; and physicians must maintain identified records on the dispensing of dangerous drugs for at least 3 years, and these records are open to inspection by authorized law enforcement officers. Kaiser-Permanente must also file certificates of death, live birth, and fetal death where the 20th week of gestation has been reached. The birth and fetal death certificates list the father's occupation, and the birth certificate has both parents' social security numbers. Some Kaiser facilities also report the identity of patients with malignant tumors to the California Tumor Registry, but this is voluntary.

Though such duties are generally performed, they are not always done. However, Kaiser personnel could not recall any physicians being harrassed or prosecuted for not meeting any of these legal reporting requirements.

In addition to these public reporting exceptions, the courts can subpoena all or parts of the medical record. The California Medical Association rules on confidentiality, which Kaiser generally uses as a guide, includes the following policy on court demands:

"The mere receipt of a subpoena does not necessarily justify disclosure, without further permission of the patient, of private information. Since the patient may sometimes be able to assert the physician-patient privilege notwithstanding the existence of a subpoena, the hospital should, whenever possible, alert the patient of the subpoena and of the time and place of hearing (unless the patient is a party to the action and has therefore already received notice) so that he may make timely objection to the disclosure."

However, in practice, Kaiser does not follow a policy of notifying patients in advance of subpoenas, and nothing in the subscriber's agreement warns patients that their records may be given to various government agencies under compulsory reporting requirements, or subpoenaed by a court.

The above policies as to confidentiality and disclosure apply to all hospital records, whether manual or computerized. When the pilot project was started, Kaiser adopted a rule that "each Patient Computerized Medical Record in the computer center is subject to the same regulations governing release, privacy, and confidentiality as is a record in the hospital medical chart room." In addition, some special regulations were adopted by the Hospital Records Committee to safeguard computerized records.

All terminals were opened and closed by action of the computer operator only. The emergency room terminal,being the most vulnerable, was placed in a restricted area and the terminal operator there had to know a valid 5-digit number to operate it. Other terminals required the use of a plastic card, and a comprehensive card-and-key system was contemplated for the future. Each terminal contained only the data prescribed by the program controlling that terminal. For example, the typewriter terminals in the San Francisco outpatient pharmacy were activated only by the computer operator in Oakland who started the pharmacy function program. "Only data entry and data retrieval as programmed in the pharmacy function was available at the pharmacy remote location terminals," and this was via private (not dial-up) telephones.

When the emergency room terminal was in operation, the Medical Methods Research group instituted an audit trail. Each request was logged, and the log was published every morning. Although designed as a security measure, it was used more as a study of utilization patterns. Dr. Collen says that it became necessary to prevent data being collected by one research project from being taken by other groups before the original group could publish its findings.

The Hospital Records Committee is responsible for new policy decisions affecting computer confidentiality. For example, initially when the Emergency Room received a record of patient visits, psychiatric visits were included on the list. Members of the psychiatric Department brought the issue to the Committee, protesting that this data should not be available to non-psychiatrists. The Committee agreed and excluded this information from the emergency room terminal.

Manual records continue to be stored in central record rooms under the supervision of a medical record administrator. These are filed by the patient's medical record number and must be signed out under the responsibility of a physician. Psychiatric records are stored separately and special permission is required for their use. When the patient is in the hospital, the patient record is moved to the appropriate ward, where it is stored in restricted files at the nursing station.

Local civil liberties groups interviewed in the Bay Area feel that Kaiser-Permanente is conscientious about the privacy of patient medical records. They have heard of no incidents involving Kaiser.

2. Patient Access

Under California law, the patient's record is the property of the physician or hospital, and the patient has no legal right to see it. But the patient's attorney, with written authorization from the patient, must be given the record for inspection and copying. Previously, this right applied only after the filing of a legal action, but that provision was amended and now he may have access before an action is filed. Indeed, there is nothing in the statute that prevents an attorney from access to his client's record even when no legal action is contemplated.

A patient who sought to see a letter he had requested his physician to write was told by Kaiser-Permanente that it would release the letter only to his attorney, upon request of the attorney and with a release signed by the patient. The release form contained a mandatory indemnity agreement under which if the patient sued a third party, and recovered, he must reimburse Kaiser for the cost of his care.

When an attorney does gain access to a record, a monitor is always present while the attorney copies it. Mr. Sexton stated that Kaiser often tries to provide only the portion of the record they consider relevant, but if challenged, he feels they must supply the patient's entire record. He remarked that theoretically, a patient acting as his or her own attorney could gain access to the record, but he did not think this had ever occurred.

Patients are also entitled to information from the record when they need it to make a decision about future treatment. The California Supreme Court found that a physician "has a duty of reasonable disclosure of the available choices with respect to proposed therapy and of the dangers inherently and potentially involved in each."

Most physicians and medical administrators are not enthusiastic about patient access to records, and the staff at Kaiser-Permanente adheres to the accepted professional view. Mr. Sexton says that Kaiser-Permanente does not allow patients access "principally because it's a nuisance." Patients don't understand the record, he believes, and the physicians then have to interpret it, which they "don't have time" to do. In addition, "unnecessary questions are raised in the patient's mind." Sexton added that Kaiser is "particularly circumspect about giving out medical information" because their great size and visibility make them vulnerable to malpractice suits.

Kaiser-Permanente patients have seldom asked to see their own records; this occurs perhaps once every six months. The "patients' assistance" personnel Kaiser has in each facility recently circulated a form asking patients to list their complaints, to see which ones arise most often. No complaints about lack of access were listed. Interviews that this project conducted with a small group of Kaiser subscribers confirmed this situation; none of them had ever requested access to their records, though all were under the mistaken impression that if they did ask to see them, permission would be granted.

Termination of the Kaiser Project - and Future Prospects

At the height of its use, in 1973, the HEW grant for the pilot project (which accounted for half its funding) was terminated, to the surprise and dismay of Kaiser officials and many computer experts throughout the country.

Because the Kaiser Foundation Health Plan, which had put up the other half of the money, was not able to absorb the extra costs, much of the system had to be dismantled. Some of it has been preserved on several minicomputer systems for discrete functions; automation of laboratory tests is continuing in a limited way by funding the Santa Clara facility with a $350,000 laboratory project and the pharmacy system has been given funds by the Kaiser Family Foundation. But the on-line computerized records, reports to the emergency room, and delivery of records via terminal to the facilities have been ended. Dr. Collen hopes that sometime in the future the separate systems that are in operation may be linked together, and they have received a grant to study the requirements of each mini-system and the criteria to connect them.

There are varying opinions as to why HEW funds were cut off. Dr. Morris E. Collen, Director of Medical Methods Research, believes it was primarily "a question of economics." He also noted that computer technology is not a current priority in the medical field in this country, and expressed the opinion that the present climate for research and development in computer operations in hospitals "is the worst in the past ten years." In addition, the difficult financial climate was complicated by the Nixon Administration's impoundment of health appropriation funds. This created a situation in which the question was not whether cuts would be made, but only where they would be made.

Several other computer scientists in the health services field explain the cut-off with additional reasons. Though its multiphasic screening program is seen by some medical specialists as a highly-valuable system whose benefits would take a decade to measure objectively, critics say that Kaiser failed to offer convincing documentation that its multiphasic screening program was reducing illness among Kaiser-Permanente patients. The system proposal also promised a more advanced and more highly implemented patient data base system than Kaiser-Permanente was able to deliver, and reviewers may have felt the project should have accomplished more than it had at the time the grant was dropped. Supporters of the Kaiser project saw HEW's action as representing an insufficient appreciation of how much time-and money-it takes to innovate in hospital computerization beyond the well-established administrative and laboratory applications.

One aspect of the Kaiser patient record project that did not draw criticism was its policies and procedures for insuring confidentiality and security of patient data in the system. In fact, the protections developed by Kaiser have been adopted by other advanced hospital projects. On the other hand, Kaiser's policies as to informed consent and patient access to his/her own record were not affected by computerization; these remain matters of medical and social policy on which Kaiser's policies reflect the mainstream of current medical opinion.

Observations

Informed opinions differ as to why the Kaiser project did not accomplish as much as its sponsors had thought they could. There were problems with hardware and software, resistance from some medical staff, and funding delays and uncertainties that derailed schedules. But a recent paper by two experts working in Kaiser's Santa Clara project, Robert Harrington and Con Korenoff, suggests that "the current barrier in medical information systems is conceptual rather than technical."* Financial applications were adopted by hospitals from the industrial models, and laboratory applications from the processing of large amounts of numerically coded data. But the patient record application, they note, poses the problem of documenting how medical professionals actually practice, and organizing a mixture of facts, observations, and speculations into a record that physicians will need--and use-- at a future date. There are presently no clear conceptions about how to do that.

Their comment underscores the fact that even at Kaiser--where many of the physician roles and rewards are more preventive-health oriented and less individualistic than in most hospitals--the question of exactly what medical professionals now do, and what they would be willing to do in the future, is at the core of any effort to extend computer use into direct patient care. Dr. Lawrence Weed has noted that computerization is threatening to doctors because they have traditionally been paid for using their memories, and a computerized system institutes "a different set of rewards, and requires sharing of power with other health professionals."** In addition, a computer system introduces a discipline that many doctors and nurses do not want to accept, and against which they can always invoke the argument that "attending the patient comes first."

Thus the Kaiser experience shows that we are barely ready to start applying "central data base" concepts to the hospitals. American society is reconsidering how health care should be organized today, whether for a subscriber group, regional population, or as a national "system". Given the mixture of personnel facilities, and technological resources available for the effort, it is not yet clear how patient information can best be collected, stored, and used in support of the total health-care system. In terms of citizen rights issues, this means that if we are ready to do so, there is still time to pay attention to citizen rights concerns at the blueprint stage of hospital information systems, rather than to have to rush into action later, as an afterthought.

---

* "A New Look at Ambulatory Health Information Systems," Information Technology for Public Services Engineering Foundation Conferences, Sept. 15-20, 1975, Asilomar, California.

**Comment at NBS Conference reviewing this report, September 16, 1975.

SOURCES

Part of this profile is based on a site visit made by the Project on Computer Databanks of the National Academy of Sciences to Kaiser-Permanente in San Francisco and Oakland in 1971, and written up in Alan F. Westin and Michael A. Baker, Databanks in a Free Society (N.Y.: Quadrangle, 1972), 205-214. A return site visit for this project was made by Alan Westin and Helene Toiv in the summer of 1974, and contacts to up-date the profile were maintained through January of 1976.

The Kaiser project has generated a large literature. The most useful items for our purposes were: Morris F. Collen (editor), Hospital Computer Systems (N.Y.: John Wiley, 1974); Douglass A. Williams, "Kaiser-Permanente Information Systems: A Review and Evaluation," in Russell C. Koza (editor), Health Information Systems Evaluation (Boulder, Colo.: Colorado Associated University Press, 1974), 283-299; Lou S. Davis, "A System Approach to Medical Information," Methods of Information in Medicine, January, 1973; J.F. Terdiman, E.E. Van Brunt, Lou S. Davis, and M.F. Collen, "A Pilot Computer System for Health Care Delivery to a Community," Medinfo 74, Preliminary Proceedings, 477; and Gerald A. Giebink and Leonard L. Hurst, Computer Projects in Health Care (Ann Arbor, Mich.: Health Administration Press, 1975),168-174.

For personal interviews, we are grateful to: Dr. Morris F. Collen; Dr. Joseph F. Terdiman; Mr. Lou S. Davis; Mr. James Sexton; Mr.James Lane; and staff members of the Northern California chapter of the American Civil Liberties Union.

CHAPTER 8. THE U.S. INDIAN HEALTH SERVICE

The approximately 850,000 Indians in the United States are part of American society, but not quite. The majority of them live on reservations as wards of the federal government, under a complex mixture of federal and tribal law. Indians are at the bottom of the nation's economic ladder, with average yearly incomes only half that of the white population, and without the upward mobility that other racial minorities have begun to achieve. In terms of health, Indians are far worse off than whites and blacks; despite dedicated efforts by personnel of the Indian Health Service, facilities and services of IHS are so bad that they have been called, without much hyberbole, "an American travesty."

Because Indian health is a responsibility of the federal government, growing out of earlier treaty guarantees, the Indian Health Service has had a chance to bring advanced computer and communications technology to bear on these problems; the Papago Indians' computer project we will examine is regarded by many as one of the most advanced problem-oriented record systems in existence today. What effect it has had on the quality of health care in its area and its chances for increased use throughout IHS are issues we will be considering here. We will also be looking at citizen rights issues in terms of some different conceptions of privacy among Indians than those held by the rest of the American population.

Indian Health Problems

The 1970 Census reports that there are 827,000 American Indians, including Alaska Natives, Eskimos and Aleuts. The health statistics below come from studies of the 500,000 Indians living on reservations. The Indian Health Service (IHS) says that it has little information about the health conditions of the remaining Indians who live off-reservation, since it is only very recently that the Service has begun to provide Indian health care centers in urban areas. Because of the continuous shifting of Indians from cities to reservations and back again as employment opportunities increase and decrease, and as culture conflict creates pressures on Indians to accept or reject reservation life, IHS believes that the health situation of on and off-reservation Indians is very similar. It is a grim picture.

The Indian death rate from tuberculosis is almost five times higher than in the rest of the population; from intestinal diseases (gastritis, colitis, etc.) almost four times greater; from influenza and pneumonia about twice as high; from post neonatal diseases (infants one month to one year old) more than four times as high. The accident death rate is more than three times as high, of which a major ingredient is motor vehicle accidents thought to be associated with alcoholism. In this connection, Indian deaths from cirrhosis of the liver are more than two and a half times higher than the rest of the population.

The over-all age-adjusted death rate for Indians is 40% higher than the rest of the population, even though significant decreases in deaths from certain diseases such as tuberculosis, influenza, and pneumonia have occurred in the past twenty years. While there has also been improvement in the rate of Indian infant deaths, the death rate for new born infants is still 23.5 per 1,000 births for Indians, compared with 16.8 for whites and 19.2 for the total population. Meanwhile, the Indian morbidity rate (illnesses) continues to rise sharply, especially for strep throat, influenza and pneumonia, and otitis media (a disease of the middle ear that can cause deafness). Dysentery is 54 times more prevalent among Indians than non-Indians and syphilis four times more prevalent. The morbidity rate is higher today for Indians than for any other population group, and in every single reported classification.

Special Aspects Of Federal Health Care Delivery To Indians

Indians are wards of the government, and the federal government undertakes to provide directly for their health care through the Indian Health Service, an agency of the Public Health Service, which in turn is a division of the Department of Health, Education and Welfare.

Placement of the IHS under HEW reflects the conflict between those who would integrate Indians into the American mainstream, and those who would preserve tribal culture. When the Indian Health Service was established in 1921, it was part of the Bureau of Indian Affairs of the Department of the Interior. By the 1950's the health of the Indians had deteriorated so alarmingly that the Hoover Commission recommended that it be put under aegis of the Public Health Service because "Indian Health Services would be under direct medical supervision, which was not the case with the Bureau of Indian Affairs, where the supervision lay with agency superintendents and others who were not medical professionals...."

The transfer to HEW was made in 1955. Despite Congressional leanings toward termination of special Indian programs, IHS has grown rapidly since then--from a staff of 2,900 and a budget of $34.5 million to a present staff of 7,400 and a budget of $200 million.

The Indian Health Service program is carried out through a system of 51 hospitals (ranging in size from 6 to 276 beds), 77 health centers, and more than 300 health stations and satellite field clinics. Additional medical and dental clinics are held at appointed locations on a regular daily, weekly or monthly schedule. Special clinics are held intermittently as needed. IHS also conducts health examinations, immunizations and health educational programs in reservation schools run by the Bureau of Indian Affairs. In addition to conventional health care, IHS operates several special programs. Among them are nutrition, maternal and child care, family planning, and sanitation.

However, measured against other health care provided directly by the federal government, in Veterans hospitals for example, or against programs funded by the federal government, or against private medical care, the staffing and facilities in the Indian Health Service are woefully inadequate. A study conducted by the Senate Permanent Subcommittee on Investigations in 1974 revealed that of 51 hospitals maintained by IHS, 29 cannot meet the certification standards of the Joint Commission on Accreditation. By contrast, the 171 hospitals run by the Veterans Adminstration are all accredited. Thirty-five of the Indian hospitals do not meet fire and building code regulations.

The Senate Subcommittee found Indian Health Service workers to be "an extraordinary group of deeply committed, hard-working people...We found them providing care in crumbling, ill-equipped federally owned buildings. We found doctors working 80 hours a week. We learned of a nurse who collapsed from fatigue and heat during patient childbirth in an unventilated delivery room. We found staff shortages so severe that entire wings of hospitals had to be closed."

The Senate investigators reported that in one hospital there was a "backlog of 1,500 surgeries needed to repair the damaged eardrums of children suffering from otitis media...some Navaho have been waiting ten years for surgery." One IHS doctor told the investigators: "We see people die of treatable, curable diseases. We see people die of diarrhea, diabetes, infections, rheumatic heart disease, typhoid fever, diphtheria... These would not be tolerated anywhere else in the United States. Here it is a way of life."

In addition to understaffing, there is the separate and chronic problem of high staff turnover. During the Vietnam war, the IHS was staffed largely by doctors who preferred the Health Service to the draft. They would serve the required two years and then leave. IHS foresaw an even higher turnover with the end of the draft.

The high turnover of doctors and other professionals, and the lack of training, fosters a lack of uniform procedures and record keeping. It also means that there is not the time to develop good communications among the various professionals—social workers, sanitarians, physicians and health workers—who deliver health care to the Indians.

Contract And Third-Party Medical Care

In places where there is no Indian Health Service facility or health facility, the IHS contracts to pay for health care given to Indians by outside hospitals and physicians. It has made such contracts with over 500 private and community hospitals, with 20 State and local health departments, and with 1,000 physicians, dentists and other health specialists.

Where there is no contract medical care available, Indians are theoretically entitled to the same medical benefits as other citizens: participation in Medicaid, and other federal state and local programs available to low-income citizens, including treatment at public hospitals. But Medicaid and other state-administered programs do not consider themselves responsible for Indian health care. Indians were not calculated either by HEW or the states as among the consumers of such services when they were first budgeted, and some states deliberately did not inform Indians that they were eligible for them. A law suit recently brought by a group of Indians in Arizona has forced belated notification, and threats of further suits may speed up the process in other states.

An Indian seeking treatment in a public hospital is likely to be turned away with the excuse that IHS facilities must take responsibility for his or her care, even though there may be no such facility within hundreds of miles. As to Medicare, IHS will not pay for the monthly premiums out of its contract-medicine budget. It argues that it can only pay for care that is actually given, and not for premiums against the possibility that care might be needed. The same holds true for private health insurance premiums.

Indian Health Boards

Most Indian Health Service Unit Areas have Indian Health Boards composed of tribal members who advise IHS on medical policy and programs. In some areas, the Board has been functioning for a number of years, and its members have acquired some background in health problems. In others, the Boards are just being created. Some health

Boards have well-defined functions, such as evaluation of IHS from a consumer point of view; handling individual consumer complaints; monitoring IHS contract programs, etc. Other Boards limit themselves to interpreting IHS programs to the rest of the Indian community.

Since the Health Boards do not have officially defined functions and there are no mutually agreed upon guidelines, a great deal depends not only on the Board's perceptions of its role, but on the IHS staff's willingness to cooperate with the Board, and its sensitivity to Indian customs and culture. In some Service Units and Area offices, there is a warm feeling of trust and mutual cooperation; in others, the relationship is a pro forma affair with little real inter-change; in still others, there is outright hostility.

Problems Of Distance And Mobility

The Indian Health Service compares its health care to that delivered in ghetto health care programs. This is true in the sense that both encounter the diseases of poverty. But the delivery of health care to Indians is complicated by their isolation —a relatively small population in a vast area with hundreds of miles of unpaved roads that are often impassable in winter. The Navaho reservation, for instance, on which 130,000 Indians live, is the size of West Virginia. In some parts of this reservation, the nearest hospital is 80 miles away, there is no ambulance service, and many people do not have any other form of transportation. In addition, many Indian tribes are migratory. The constant shifting of population on and off the reservation has already been noted. But Indians on the reservation also migrate within it, following seasonal agricultural and employment opportunities. According to V.H. Chadwick, Deputy Director of the IHS, many Indians "will visit not a facility, but facilities across the geography we serve...Some Indian people...have as many as six or more Social Security numbers because it is easier to get a new number than it is to carry the old one with them..."

Record Keeping Problems

All of the problems outlined above mean that the Service is forced to practice crisis medicine, dealing only with the patient's chief complaint at the moment. Thus, if a patient arrives at a health facility with a cut on his wrist, the attending physician will in all likelihood give him a tetanus shot, place a bandage on the cut and tell him to come back in a few days if he is not feeling better. The doctor will not learn that the patient is a diabetic, and is past due for a refill on his medications, that he may have a chronic heart condition, or that he may have a history of suicide attempts, which would certainly give a special significance to the cut on his wrist.

While there have been attempts to begin multiphasic screening programs, they have been abandoned for lack of resources. According to one IHS official, "You spend a lot of time (with multiphasic screening) seeing healthy people which would be better used dealing with illness."

Although much health data may have been collected on each patient by various health professionals, the patient's record may be scattered in the various health facilities he or she has visited, or it may have been collected by a social worker or sanitarian and there is no system for making it available to the doctor. No integrated set of data exists for each patient, and thus each provider of health care must treat the patient with the benefit of only that data which he or she alone has collected.

The problem of maintaining useful medical records is further complicated by the language barrier. In the Papago Indian tribe, for instance, 65% of the Indians do not speak English and it is difficult for staff members to elicit meaningful health information from the patients. This problem is further exacerbated by the fact that with the end of the Vietnam War, foreign doctors have largely replaced those doctors who served in lieu of the draft. While many Indians who do not speak English can understand basic English, they find it impossible to comprehend the Phillippine, East Indian or Pakistani doctor, whose own accent or mastery of English is sometimes shaky.

Computerization Of Records

All of these considerations led the IHS to turn to computerization projects for some possible solutions to its record-keeping problems. Since 1968, IHS has pursued two approaches to computerization. The first of these was the implementation of an automated system in Albuquerque, New Mexico, designed to assist management decision-making at all levels of the IHS program. The fundamental output of this system is batch-processed reports that focus on over-all statistics of facility utilization, inventory, personnel and the nature of services provided (immunizations, dental services, etc.) to various Service Units within the Indian Health Services. These off-line reports are used by IHS directors in the field and by IHS officials in Washington to help in planning budgets and deployment of resources.

The second approach, on which we will concentrate, is the Health Information Service (HIS), established in Tucson. It is a pilot project which creates integrated, on-line health records on the 10-12,000 Papago Indians in Southern Arizona who are served by the Sells Service Unit of the Indian Health Service.

The Sells Service Unit consists of an integrated health care team of physicians, public health nurses, sanitarians, social workers, mental health workers, and includes contract health services as well as the tribal health program.

The area that the Sells Unit serves is characteristic of the reservation conditions already described. The main Papago reservation is as large as the State of Connecticut, with only 6,000 people living on it in fifty small, scattered villages, with few telephones and fewer roads. An additional five to seven thousand people live near the reservation or on the nearby San Xavier reservation. The Sells Unit has a 50-bed hospital located at Sells in which outpatient clinics are also held. There is an outpatient clinic at Santa Rosa and another one at San Xavier. In addition, intermittent field clinics are held in various locations such as church buildings one or two half days a week. There are major areas without electricity and running water. About 65% of the houses are substandard.

The main function of the computer is to provide health professionals with a complete medical summary on each patient, which can be retrieved every time the patient visits any of the clinics, outpatient stations or the hospital in the Sells Unit. Health professionals are given an encounter form on which to write down patient information. This information is fed into the computer and can be retrieved instantly any time the patient visits any facility again. The filling out of the encounter form itself has assisted in more systematic record keeping. According to Dr. Rice Leach, Director of the Sells Unit: "The encounter form provides a terrific reminder to doctors to write down what they have been taught to write down since the first day of medical school...We know a lot of things we are supposed to write down, but if the reminder is not there in front of you, it slips your mind."

The on-line patient records are made available through remote printer terminals which are linked to the computer by telephone lines and are located at each of the health facilities. Field personnel are equipped with portable terminal devices which can operate over any standard telephone headset.

The medical summary provides the health care team member with a brief, multidisciplinary health profile on each patient. The computer generates the summary within a few seconds of receiving a request from one of the remote terminal locations. The summary includes all information collected during recent patient encounters, although it takes about five days to enter new materials, so that patient information gathered during a visit within the five days past might not be included.

The data in the medical summary includes: measurements; active and inactive problems; active medications; inpatient, outpatient and field encounters with diagnoses and a health status surveillance component which includes immunizations, skin tests, laboratory tests, X-rays and special examinations and histories. All of these items are designed to permit the early detection of treatable health problems; to assist in the identification of individuals who are susceptible to specific health problems; and to provide the foundation for an improved patient follow-up system.

The most important feature of the medical summary is its problem orientation. The problem list is included as part of the medical summary and made available to providers of health care. The problems included may be medical, emotional, social, environmental or educational. The list allows members of the health care team to treat each patient in the context of all of his or her health-related problems, rather than treating just the current problem. Health team members make additions, deletions and modifications to the problem list by completing standard data collection forms. The data stored for each problem includes a system assigned problem number, problem code, problem narrative, dates of entry and change of status, the facility at which the problem was entered and identification of the health professional entering each problem.

Included in the medical summary, and available at each encounter with the patient, is an up-to-date list of all procedures and tests that are past due or are scheduled within the next twelve months. This permits the physician to take advantage of a complaint visit to perform much-needed preventive maintenance.

The computer can provide access to all data of a given type (e.g. all diagnoses, medications or operations) for a given patient. The response time for such retrievals is generally between fifteen and thirty seconds.

Special retrievals provide other, more complex kinds of information. The TB contact status report, for example, provides a listing of all identified contacts of an active TB patient, and for each, the date and results of the contact's last skin test, date and results of the latest chest X-ray and current prophylactic medication status.

In addition to on-line retrieval of individual medical records, the Tucson Health Information System is able to retrieve data for management and planning, for epidemiology and research. It can respond to a request like: "How many cases of these six diseases have been diagnosed among the residents of any of these eight villages, but I want only diagnoses made between April and September of 1970 for female children between the ages of eight and twelve."

These off-line records are printed on high speed equipment at the computer center and delivered to the consumer by courier. Among the scores of reports generated in this way are the following: weekly listings of scheduled encounters for each physician and public health nurse; weekly listings for each public health nurse of all patients who have had recent clinic visits in each Public Health Nurse area; monthly reports for sanitarians of the incidence of infections and parasitic diseases in a designated community; various population summaries by district, community age group, sex, etc.; incidence of disease reports; facility utilization reports by communities, age groups and time periods; reports of all children whose height, weight, or head circumference measurements exceed specified percentile values from standard curves; special reports on accidents, family planning visits, patients on selected medications, patient disposition, and other miscellaneous reports.

In addition to the above, the computer can produce reports on a specific disease, with its demographic and geographic parameters, to support specific corrective programs. Among these have been reports on: malnutrition and iron deficiency anemia; diabetes; amebiasis and dysentery; identification of deaf and blind children; identification of attempted suicides.

Citizen Rights Issues

The most important right of privacy for most Indians is the protection of tribal (community) values and procedures from hostile surveillance or regulation by outside authorities — whether the Bureau of Indian Affairs, local governments, or the Indian Health Service. Within the tightly-knit reservation life, much like older small-town communities in colonial America, little individual privacy is asserted against fellow tribe members. But privacy is claimed strongly when outsiders control the education, social behavior, employment patterns, or health care of Indians. Conceptions of individual privacy rights against government in the Bill of Rights framework, are also a matter of concern to many Indians. Indeed, not only were such rights of individual privacy included among those rights sought by Indian leaders to be included against tribal government violation in the Indian Civil Rights Act of 1968 but recent tribal constitutions (such as the Blackfeet tribe) specifically guarantee the right of personal privacy.

The result of these special aspects of Indian culture is that patients in the IHS system have not only individual concerns over matters of informed consent, improper revelation of embarrassing conditions, and the like but also special concerns about invasion of tribal religious and group mores. IHS officials have generally been sensitive to these concerns, but the overall citizen rights policies of IHS have — until recently — followed about the same line as other medical institutions in American society, governmental or private.

When the Health Information Service computerization program became operative in 1969, the Papago Indians did not have an Indian Health Board. The Board, called the Executive Health Staff, was not created until 1972. Therefore, the IHS staff dealt directly with the Papago Tribal Council. They conferred with the Council about the computerization program the IHS Office of Development had in mind, explaining "the information that would be made available and the ability of the program to maintain the confidentiality of all parts of it." "No matter how long it took," Chadwick recalled, "we waited until the Indians fully comprehended the computer and then requested that it be used." IHS officials also allayed fears that computerized records might dictate culturally unacceptable medical procedures. Dr. Leach states: "If the computer tells me that an 85 year old lady needs a very personal examination, and she doesn't want it, she doesn't get it unless it is a life-threatening or urgent situation. We don't treat the computer..We treat the patient."

In 1972, when the Papago Tribal Council authorized the establishment of the Executive Health Staff to act on behalf of the tribe in initiating, coordinating, administering and implementing tribal health program, the IHS made its presentations about health operations, computerized and manual, to this group.

According to Chadwick, the Indians residing on the Papago Reservation know "all there is that it is possible for them to consume" about the Health Information System. The Health Executive Staff is periodically briefed by IHS officials in Tucson about the system's operations and the Papagos are then informed of the main points by word of mouth.

1. Patient Access

Prior to passage of the Federal Privacy Act of 1974, policies on patient access to medical records and confidentiality were governed by the Indian Health Manual, Chapter 3-Health Records. This 90-page chapter, distributed to all Service Units and Area offices, elaborately detailed every aspect of medical record keeping in the Service. Its policy on patient access was:

"At no time should the patient or the patient's family be permitted to review the health record. The patient should be referred to the Service Unit Director, who, under proper and appropriate circumstances, may provide some information to the patient."

The manual adopts the standard medical position that the record is the property of the facility and the IHS.

What the actual practice was is not easy to determine. On the one hand, E.S. Rabeau, a senior IHS official, reported that patients were generally permitted to see a copy of their records "as a matter of course." On the other hand, Mozart Spector, Director of the Office of Program Statistics of IHS, and Howard Walderman of the PHS General Counsel's Office stated that a patient who "pressed hard enough" could usually see his or her record.

HEW regulations implementing the Privacy Act provide that "Any individual may request notification of or access to a medical record pertaining to him." The individual is to be given direct access "if the responsible official determines that direct access is not likely to have an adverse effect on the subject individual." If this is the determination, the medical record will be sent to a "designated representative" of the individual, "a physician, other health professional, or other responsible individual." Such person is then allowed "to review the record" and make the decision whether to reveal "its contents" to the individual.

This new access policy has been described in posters displayed in IHS clinics, though access is not mentioned in the "Statement for Maintenance of Health Records" that IHS now gives each patient to sign when obtaining information from him or her. (This statement will be discussed later under "Confidentiality"). As of late 1975, IHS officials report, most access requests have been from IHS employees wishing to see their personnel records. Reports were not yet in as to patient access requests.

There have been complaints from some regional personnel that they are not qualified to decide whether giving a patient a record would be detrimental, and the Service Unit Directors have been authorized to seek assistance from a physician when necessary. Some problems have arisen because the regulations are designed primarily for situations in which the government is not the primary care provider. For example, there is usually no other physician, outside the IHS that can review a patient's record if there is an access question.

Should errors be found in patient records, IHS has taken the position that it will add corrections to the record rather than wipe out the old information that is there. The same policy has been adopted by the National Institutes of Health.

2. Confidentiality

Prior to the Privacy Act, regulations for protecting the confidentiality of patient information and records were listed in 20 closely typed pages of the IHS Manual's Chapter on Records. In general, records could be shared without patient consent among IHS health professionals for the purpose of providing direct patient care; for statistical research purposes; within the Public Health Service for audits by the General Accounting Office; and in cases where the U.S. Attorney is engaged in defending the PHS against a patient's claim. Law enforcement agencies such as the FBI, and local and tribal police could be provided with non-confidential identification information (name, age, height, weight, color of hair, etc.) without patient consent. Release of confidential medical information to law enforcement agencies required signed patient authorization.

Release of patient information to contract physicians and hospitals, social agencies, insurance companies, employers, attorneys and tribal authorities required signed patient authorization. Release of patient information for research outside the Public Health Service was not permitted. Patient records were released when subpoenaed, with the patient required to be notified promptly.

In the past, IHS received quite a few requests for patient information from prospective employers and from government agencies. One government request came from an assistant U.S. Attorney, who demanded that IHS officials provide him with records of all Indian women under the age of 18 who had contracted venereal disease. He wanted to learn from these women the identities of the men who had infected them and prosecute them for statutory rape. Despite his pressure on the Justice Department and on HEW, the IHS refused his request. "We're not policemen, and we're not in the tracking business," observed Sidney Edelman, Assistant General Counsel of the Public Health Service.

Another request came from the U.S. General Accounting Office (GAO) a few years ago. A GAO official asked IHS for 300 medical histories of Indian women who had been treated for gonorrhea along with their names and current addresses. He said that as part of an "environmental study" GAO wanted to visit these women and investigate water, soil, and air conditions in their home areas. The IHS official refused, saying that such epidemiological studies had nothing to do with the auditing and fiscal functions Congress had assigned to GAO, and there was no justification for supplying the case histories. This set off a series of strong demands by higher and higher officials at GAO. Finally, the IHS official sat down with a top GAO executive and patiently explained the problem to him. "If your wife had contracted gonorrhea and had been treated at a federal hospital," he asked, "would you want some federal official coming to the door and announcing that he wanted to talk about how she got it?" The GAO executive saw the point, apologized, and the incident was closed.

Employer requests for medical information have been referred back to the patient for specific release authorization. Dr. Leach states that "when an employer comes directly to me for information (without patient authorization), I send him home."

Complaints about breaches of confidentiality seem to occur mostly about people who have jobs that give them access to medical records who are also residents of the community. According to a doctor at the IHS hospital serving the Apache tribe: "This is a small town and people tend to gossip about information they see." The doctor confessed that he himself had used patient medical records in a non-professional way. He looked into medical records when he and his wife were looking for a new babysitter because they had been "burned" by a babysitter previously, and they wanted to check on the candidates. Another incident related by the doctor concerned someone who applied for a job at the hospital who had been an emergency room patient. The doctor told the nurse to look in the individual's chart, and after doing so, the nurse said "she didn't want to hire him."

All of the above incidents refer to the manual records which are kept in addition to the computerized records. When the HIS system was about to become operational, Papago Indian leaders expressed the fear that they would be "put on public display if their medical records were computerized." IHS officials convinced the Indians that confidentiality would be better preserved under an automated system than under a manual one. It's far safer to have that sensitive information locked in a computer, than to have a record just lying around for anyone to see," an IHS official explained to the Indian representatives.

In his 1972 testimony before the HEW Advisory Committee on Automated Personal Data Systems, Dr. Leach explained the security measures taken to protect computerized information. "The files are locked and you need a lock number to get a medical summary." The system protects against an individual conducting a fishing expedition for other information such as "Gee, I wonder if Cousin Charlie has got his problems listed."

In addition, the system is developing a unique internal numbering system which is seen as a further aid to preserving confidentiality. The numbering system was not developed for the primary purpose of insuring confidentiality, but to deal with the fact that only 20% of the Papagos have Social Security numbers, and many of these may have more than one. In addition, Papagos, like most Indians, have an Indian name, which they do not share with outsiders, and they may have a variety of English or Spanish names which they don't regard as important and so sometimes use one or another of them. The computer will sort out these various names against the other identifying information, to create one record for them all which will be assigned a special number.

After the federal Privacy Act went into effect, in September of 1975, IHS gave each patient a copy of a "Statement for Maintenance of Health Records." This explained the statutory authority under which IHS maintained such records. Then the form explains:

> The purpose for requesting personal information is to maintain an accurate record of your medical care. This record contains what you tell the Health Care Provider is wrong with you or how you feel. The health care providers write into your record your family and personal history and the results of your physical examination. They also record the results of all tests, medications, treatments, or surgical procedures you receive in Indian Health Service facilities.

> With few exceptions Indian Health Service personnel will not tell anyone what is in your record without your written permission. Copies of your record must be released to the State and Federal courts if we are ordered to do so. Information from your record is used to report medical conditions to Federal, State and local agencies, including schools, Tribal groups, and health departments if they need to know the information. It may be used to send needed information if you are referred outside the Indian Health for additional care, to evaluate the care you receive, to determine professional certification and hospital accreditation, to publish statistical reports, and to plan special health programs.
>
> You may choose not to answer the questions if you so desire. However, this could have a direct impact on the quality of care you receive. Therefore, it is in your best interest to provide complete and correct information so that we will be able to carry out our responsibility of providing you proper health care.

Following this is the statement "I Understand Why The Information is Asked and the Purposes and Uses of This Information," with a place for the patient's signature and the date. The HIS computer has been reprogrammed so that it shows whether a patient has seen and signed the Privacy Act statement.

Public health officials and IHS officials in the field have already spent considerable time and money on implementing the 1974 Privacy Act, including a week-long training session in Washington and local meetings attended by Indian groups and IHS personnel. Although IHS people feel that the general idea of the Act is a good one, they complain that not enough thought was given to the special complexities of medical records, and that some of the requirements are burdensome and confusing.

The most burdensome requirement, they feel, is the disclosure log in which an entry must be made every time patient information is disclosed, stating the date, nature and purpose of the disclosure, as well as the name and address of the recipient. James McArthur, the Area Privacy Coordinator at Sells points out that there is a total community program that carries health into the field. It is common for IHS personnel to consult with county nurses and school health workers, and every instance of this sharing is required to be noted. IHS public health nurses find the requirement burdensome too, and practices such as reporting positive strep throat cultures to school nurses may have to be curtailed unless additional personnel are hired, according to Spector and Walderman. In addition, IHS has had difficulty in obtaining from the Social Security Administration information it obtained previously to determine eligibility of Indians for benefits under other government programs.

Future Of The Computer In The Indian Health Service

The computerized HIS system is regarded with enthusiasm throughout IHS. Mr. Chadwick calls it the "leading" computer-based health information of its kind. The National Indian Board of Health voted unanimously to adopt HIS throughout the Service. Area directors throughout the system are also favorable and the system has won almost universal acceptance from the physicians and patients among the Papagos. "Doctors at Papago scream if the computer is shut down for 24 hours," Mr. Chadwick observed.

A brief experimental program in Alaska was also enthusiastically received by officials there. Using a telecommunications satellite that was located there for a period, it was possible to conduct two-way television and long distance specialist consultations. The retrieval possibilities were not as great as in the Sells Unit, but officials in Alaska would like to see the project continued. Throughout the IHS, officials are working on computer possibilities. In the Billings area, the Chief

Medical Officer is chairing a committee to determine their computer requirements. Special HIS advisory committees are trying to develop special computerized high-risk programs(alcoholism, suicide attempts, maternal and child health, etc.) to improve IHS ability to allocate resources. Other plans call for the improvement of data entry through the use of video display stations at field sites, and the development of reporting systems for social service workers, mental health workers and other paramedical groups.

But in spite of all these dreams, it is unlikely that the Sells Unit will be expanded to include more functions, or that other units and areas will be given computers. An indication of that unlikelihood is in S. 522, the bill to expand the services and facilities of the Indian Health Service. The bill proposes to expand the Service's budget substantially, including a separate large construction budget to build new hospitals and other facilities over the next five years, and making provision for funding health services to urban Indians. There is no budget item in this bill for an expanded Health Information System. According to Chadwick, a HIS system throughout the Indian Health Service would cost between five and seven million dollars, and it would be "a hell of a good investment." But Congressional supporters of IHS did not write in funds for such computer expansion.

Observations

The HIS experiment with the Papagos Indians has indeed proved that it can create integrated, instantly retrievable medical records that solve the formidable problems of vast spaces, poor roads, and telephone communications, the migratory nature of the population and the language barrier. It is a system that has strong support from physicians, nurses, and managers using it. It has also proved that the system can identify and document the most pressing health needs of the Indian people it serves.

But these computer capabilities merely emphasize the gap between society's ability to record and diagnose its ailments and its inability to treat them. Until the Papagos—along with the rest of the Indian population in the United States--can be assured of an adequate health care delivery system, including hospitals at least on a par with those available to the rest of the population, adequate numbers of health care personnel, adequate funding to combat their special health needs and to improve sanitation, nutrition, housing and other environmental factors that jeopardize health, Indian health will continue to be in crises. In this crisis, a computerized medical records system can only be regarded as luxury. If the needs outlined were to be fulfilled, however, then the HIS system pioneered among the Papagos could serve as the central force for making the delivery of medical care effective.

As far as citizen rights are concerned, IHS now has a new set of policies defined by the Federal Privacy Act. There would seem to be no reason why the computerized system in IHS will have any greater difficulty in complying than the manual record systems. How the new rules as to confidentiality and patient access will work in practice will be examined in 1976-77 by the federal Privacy Protection Study Commission and by Congressional committees overseeing the operations of the Act. This will provide some important data about the advantages, disadvantages, and costs of the new rights set by the Federal Act, and how the Indian population regards these measures. IHS officials interviewed in early 1976 said it would be "several years before all the contingencies are clarified." Some of the most important of these problems will be discussed in our final chapter.

SOURCES

A site visit was made to the Washington offices of the Indian Health Service in July of 1974 by Alan Westin and Richard Silberberg. Follow-up interviews, including telephone interviews with IHS officials in Arizona, Indian leaders, Indian Rights groups, and American Civil Liberties Union affiliates in the Southwestern area, were conducted during 1975, primarily by Helene Toiv. Additional interviews were held in late 1975 and early 1976 on IHS compliance with the Federal Privacy Act. The first draft of the profile was written by Silberberg, then revised and rewritten for the Final Report by Westin and Florence Isbell.

The most useful published sources for the profile were: U.S. Department of Health, Education and Welfare, The Indian Health Program of the U.S. Public Health Service, Washington, D.C., U.S. Government Printing Office 1972; U.S. Department of Health Education and Welfare, Indian Health Service Office of Research and Development, Washington, D.C., U.S. Government Printing Office 1973; Indian Health Service Health Information System: Summary Briefing, (mimeo), Office of Management Information Systems, Tucson, Arizona, August 2, 1972; "Indian Health Service System, Tucson, Arizona," in Gerald A. Giebink and Leonard L. Hurst, Computer Projects in Health Care, (Ann Arbor: Health Administration Press, 1975), 164-168; Testimony of Indian Health Service Deputy Director H.V. Chadwick before Advisory Committee on Automated Personal Data Systems, Department of Health, Education and Welfare, August 17, 1972, p.70; U.S. Department of Health, Education and Welfare, The Indian Health Service Health Information System: Summary Description, January 4, 1972, Washington, D.C. U.S. Government Printing Office, 1972, p.4; "Indian Health Care Improvement Act," Hearings before the subcommittee on Indian Affairs of the Committee on Interior and Insular Affairs, House of Representatives, 94th Cong., 1st Sess.,1975; Health Care in Alaska via Satellite,Martha C. Wilson, M.D. and Charles Brady, paper for AIAA Conference on Communication Satellites for Health/Education Applications, Denver, Colo., July 21-23, 1975; Indian Health Manual, Part 3, Professional Services, Chapter 3 (mimeo) Indian Health Service, July 12, 1972; Indian Health Service Reporting Systems, Public Health Service, Dept. of Health, Education and Welfare, Rockville, Mo. (February 7, 1972, p.1); "Hearings on Indian Health Care," Before the Permanent Subcomittee on Investigations, Committee on Government Operations, U.S. Senate, Sept. 16, 1974.

For personal interviews, we are grateful to: H.V. Chadwick; E.S. Rabeau; Charles D. Brady; Sidney Edelman; Mozart Spector; Howard Walderman; James McArthur; Cecil Williams; David Smith; and James Purcell.

CHAPTER 9. THE MULTI-STATE INFORMATION SYSTEM

The Multi-State Information System (MSIS) is an automated information system for mental patients' records, designed to serve both administrative and research purposes for participating institutions throughout the U.S. The owner and manager of the central computer, the Information Sciences Division of Rockland Research Institute, a state facility in Orangeburg, New York, does not deliver primary care or pass on any questions of eligibility or claims of patients; its role is limited to developing computerized forms, administering the data base and data communications, and sponsoring research by the Institute's own personnel. In our scheme, it is primarily a Zone 3 organization as far as its research function is concerned, but it could also be considered an extension of the Zone 1 mental health centers that use it, and it is precisely the hybrid character of MSIS that makes it important for our study.

MSIS is a system that has invested long deliberation and careful planning to assure the confidentiality of patient records. Paradoxically, this system has been publicly attacked for posing grave new dangers to confidentiality. Part of the concern of both the designers and the critics of the system stems from the especially sensitive nature of psychiatric information but part flows from the fact that it is a new type of individually-identified patient record system - a multi-state databank with each state having different statutes, practices and perceptions of the degree of confidentiality required for medical record-keeping.

Background

The genesis of MSIS was a demonstration at the Fourth World Congress of Psychiatry in 1966 by the Information Sciences Division of the Rockland Research Institute on the uses of computers in psychiatry. At the demonstration, clinical data, collected in checklist form on a psychiatric questionnaire, were converted by computer into readable narrative reports. To develop this idea of producing narratives by computer, the U.S. National Institute of Mental Health invited the Information Sciences Division to apply for a development grant, which it obtained in 1967. This was an $8 million grant for five years, and it was awarded with the understanding that MSIS was to be a regional system.

By 1974, six states--Connecticut, Massachusetts, Rhode Island, Vermont, some facilities in New York, and one facility in New Jersey, plus the District of Columbia--were participating on-line in MSIS, using the central computer at Rockland Research Institute in Orangeburg, New York. Most MSIS users are state institutions or private facilities relying on state and federal money; these serve largely lower socio-economic patients. But there are some private voluntary agencies and community mental health centers in MSIS who have middle class patients, as well as a few exclusive psychiatric clinics with affluent patients.

In September, 1975, MSIS had approximately 400,000 patients on file, most represented by a single episode of admission, treatment and termination. About 45,000 were involved in multiple episodes. At present, MSIS is the largest computer-based mental health information system in the country.

In 1972, NIMH funded a two-year renewal grant of $2 million for further development of MSIS. This money supported the staff and the central computer at Rockland, with each participating state assuming a share of the rest of the operating costs. When the federal grant ended, MSIS' 1974-75 operating budget of $550,000 came entirely from the participating states. The cost to a participating institution is $5.00 to process each patient episode from admission to termination.

How MSIS Works

The information that MSIS computers is capable of collecting and storing falls into five categories:

1. Demographic: Sex, birth date, address, marital status, ethnic group, religion, household composition.
2. Administrative: Legal status, physical location of patient or name of treating unit, prior psychiatric service, source of referral.
3. Patient progress: Clinical appraisals of patient's psychiatric condition including mental status examinations, progress reports, diagnosis, case history.
4. Treatment: A record of all treatment contacts and a detailed record of psychotropic drug therapy.
5. Service rendered: Direct services rendered, contacts made, indirect services such as consultation and community education, ancillary services such as x-ray, laboratory tests and dental treatment.

While these are the total capabilities of MSIS, the system was designed so that facilities could participate in accordance with their varying needs. Only two types of records are mandatory. The first is the Admission form, which must be filled out for each patient episode stored in the computer. However, even many of the items or this form may be omitted at the option of the participating institution; of its 37 items, only 6 need to be filled in to create a patient record. The second of the mandatory records is the form showing how the patient episode terminated (either a Termination form or a Change in Status form).

All other forms available to MSIS users are optional. Two of these optional forms of particular interest in mental health administration are the Mental Status Examination Record, which makes possible appraisal of the patient's problems and their severity; and the Psychiatric Anamnestic Record, designed to record basic case history data.

To enter patient records in MSIS, participating institutions bring their completed forms to the nearest MSIS terminal. Some hospitals and mental health centers have their own terminals; others use terminals located in other facilities or in regional or state offices. Most data collected from New York State facilities, for example, is processed on the computer of the State Department of Mental Hygiene, in Albany.

Terminal communication with the MSIS computer is by ordinary dial-up telephone lines. When information is transmitted to the computer, it generates a corresponding report which is sent back to the terminal and distributed by terminal personnel to the appropriate participating facility. When an Admission form is submitted, for example, a note reflecting the information on the form is returned to the facility. Many reports generated by MSIS are in narrative form and substitute in part for those usually dictated by clinicians. This work is done by batch-processing, not on-line, since rapid response is not needed for MSIS activity.

Clinical Uses

To demonstrate its record-keeping capabilities, MSIS has prepared a model case history for a fictitious patient named Mary Stewart. The information on Ms. Stewart was taken by clinic personnel and recorded on machine-readable forms, from which the computer produced 15 tabular and graphic summaries for her psychiatric records. It must be kept in mind, that this is an ideal representation of the system's potential; few participating facilities use all of the forms, especially the diagnostic suggestion one, although some may provide all of the clinical techniques and services illustrated in Ms. Stewart's case.

The Admission form establishes the patient's identity, assignment to ward and unit, demographic data, appraisal of problems, previous psychiatric service, and source of referral. Ms. Stewart's record shows that she is a 24-year old secretary who lives with her parents. She came to the clinic voluntarily, apparently suffering from drug intoxication. She had previously received psychiatric care from a private psychiatrist and at a mental health center. Among her recorded problems were disturbances in her relations with family and other people and in job performance, as well as suicidal thoughts, depressed mood, social withdrawal, delusions, hallucinations, sexual problems and incoherent speech. The diagnosis was drug or poison intoxication and the overall severity of her condition was judged slight.

Ms. Stewart then underwent complete psychiatric, psychological and social evaluation at the clinic. Basic case history data was recorded on the Psychiatric Anamnestic Record form, and a narrative report was produced from this data by the computer. After verification of the report's contents, usually indicated by the physician's signature, the narrative may be placed in the patient's chart. The information for Ms. Stewart's report was obtained from a physician, the patient, and a family member, and its reliability rated as "good".

The onset of her current condition, which developed gradually and has been evident for three months, was apparently associated with a mildly stressful situation involving a drug reaction and family problems. The patient's mother has a history of a mild functional psychiatric illness; her father has a history of a severe functional illness; she has one sibling who has been at least mildly ill. The section on personality traits reports that the patient is inhibited, unable to relax, emotionally distant, stubborn, suspicious, and gets little pleasure out of life.

The Mental Status Examination Record includes detailed information about the patient's appearance, general attitude and behavior, mood, judgment, potential for suicide or violence, insight and attitude toward illness, and overall severity of illness.

Based on the information in these two forms, the computer can produce a suggested diagnosis. This, however, is solely a tool for the clinician and does not become a part of the patient's record. For Nancy Stewart, the computer gave two most likely diagnoses: schizophrenia, paranoid type, and drug dependence, hallucinogens. A recent study at MSIS has shown a high correlation between the computerized diagnosis and the doctor's diagnosis, but as already noted, few MSIS participants use this procedure today.

During the course of Nancy Stewart's outpatient therapy, her condition deteriorated, and she was transferred to inpatient status. Her continued delusional thinking and suspiciousness led to the conclusion that she was schizophrenic; drug, group and individual therapy were prescribed and monitored.

Her progress was monitored on the Periodic Evaluation Record, which noted persecutory delusions, good physical health, and her activities, which included visitors and attending organized patient groups. After three months, Ms. Stewart had improved enough to be returned to outpatient status, a fact recorded on a Change in Status form. The Periodic Evaluation Record-Community Version showed that during her outpatient therapy she was still slightly suspicious and uncooperative, but that her condition was improved.

Approximately six months after Nancy Stewart's initial admission, the episode was terminated. Her Termination form recorded the final official diagnosis and stated that no further care was indicated.

MSIS has also automated a problem-oriented psychiatric record designed to introduce clarity into psychiatric record-keeping by making the treatment rationale explicit. This was used in Mary Stewart's case. The hope is that structuring the record around a core problem list and keying all treatment and patient progress data to problems will foster increased use of the chart as a communication medium and as a tool for utilization review and program evaluation. It is still regarded as experimental, however, and is seldom used by MSIS participants.

Ms. Stewart's fictitious case study illustrates the role that automation could play in every stage of keeping individual psychiatric records. However automated clinical records are being used far less frequently in MSIS than administrative and research computer functions. There are several reasons for this. Doctors, according to Dr. Eugene H. Laska, Director of the Information Sciences Division, "are not entirely enthusiastic about record-keeping in any shape, form or fashion," and he knows of very few psychiatrists who rely heavily on patient history records, whether manual or computerized. Generally, psychiatrists are skeptical of conclusions drawn by an unknown author of a patient history or of a diagnosis found in the record. They prefer to collect and evaluate the personal data themselves. An important exception to this is the use of drug summary outputs, which enable a doctor to find out which drugs have been tried and in what dosages, and whether or not they have been successful.

Dr. Laska notes, however, that younger doctors at Rockland Psychiatric Center are pro-MSIS because it takes care of many of their record-keeping chores and allows for useful retrievals. They are not hostile to computerized diagnostic suggestions, and use of the Mental Status Examination Record by doctors there is increasing. But

Dr. Laska adds, he does not really know "if the outputs are being read."

At the Connecticut Mental Health Center--which MSIS officials suggested for a field study because it is a heavy MSIS user--MSIS was planned only as an administrative aid, and not for clinical purposes. The Connecticut Mental Health Center at New Haven is a joint venture of the State and Yale University. It is largely an outpatient facility with only 45-50 inpatient beds. The Mental Status Examination Record is used only for utilization reviews on the inpatient wards. Clinicians prefer to use the notes they dictate and that are put into the patient's chart; they believe that the MSIS forms are "not rich enough for them."

Research Uses

Aside from physicians' instinctive preference for their own notes, and their traditional dislike of record-keeping, a less explicit element may influence the greater research and administrative use of MSIS capabilities. Along with other mental health information systems, MSIS was originally supported by research-granting agencies, as a research tool. The grant receivers tend to be more responsive to the research-granting agencies than to the service-providing agencies.

The research capability of MSIS has been impressive. For example, researchers have investigated drug data in an effort to link variables from an individual's background to drug response. A study using data on 9-10,000 patients at Rockland Psychiatric Center examined the relationships among drug prescriptions, diagnoses, and other variables. The study showed that in many cases, the optimal drugs were not being prescribed.

A research team directed by Dr. Carole Siegal, a mathematician at the Information Sciences Division, recently developed a way of evaluating the effectiveness of community health center procedures. The study showed that there were differential service patterns for various age, sex and ethnic groupings, and raised questions as to the justifications for this.

Research and program evaluation activities using MSIS data are particularly strong at the Connecticut Mental Health Center, whose staff members include professors or instructors at Yale. According to Michael Levine, Chief of Statistics and Data Processing, many staff members are engaged entirely in research. More than forty papers published by the staff of this Center have been based on or have used MSIS data.

Researchers at the Information Sciences Division, as a follow-up to studies suggesting that Reserpine therapy for hyper-tension is associated with breast cancer, have started a study of this relationship using the prescription records of Rockland patients on the MSIS file. The study is particularly relevant in a psychiatric center because Reserpine was routinely prescribed as a psychotropic drug.

Administrative Uses

The greatest use to which MSIS is put is still for administrative records and reports. To serve these needs, MSIS has two basic retrieval mechanisms. GALS (Generalized Alphabetic Listor) is a language used to generate lists of patients who satisfy criteria specified by a user; for example, a list of all male patients in residence between the ages of 18 and 25 with a diagnosis of schizophrenia,paranoid type. STARGEN (Statistical Report Generator) is a language used to produce statistical cross tabulations: For example, a cross tabulation of all patients in a particular facility eligible for Medicaid by age, sex and diagnosis.

Using these two retrieval systems, MSIS has developed a broad variety of lists tailored to specific information needs: Lists of patients whose legal commitments are due to expire; patients who are due for physical examinations or other tests; patients who are receiving more than two psychotropic medications; all patients in a given building under the supervision of a particular doctor with their active drug prescriptions. (The last list is routinely used by nurses to prepare medication cup cards and by physicians to review the current regimes of their patients.) At one participating facility, this routine list indicated unusually large amounts of a sleep-inducing drug were being used. Checking revealed that one night attendant was over-medicating the patients so that they would not disturb him during the night.

MSIS allows participating facilities to comply easily with NIMH requirements for an annual report on patients in residence. To meet this need, MSIS developed several NIMH tables, as well as other tables to be used to satisfy state reporting requirements.

As users become aware of the capabilities for statistical reporting, the requests for reports both increase and become more diversified. Today, about half of the total computer time is spent on such retrievals: Local alcoholism and other clinics now get lists of patients who fail to return for follow-up visits. Rockland County Community Mental Health Center periodically requests a list of all patients who showed suicidal tendencies and who have not been seen for 30 days.

Mental health service does not generally require on-line retrieval of individual records. As Dr. Laska noted, "No one's upset if the computer is down for three hours." This is because most users keep manual records on their patients and can go to these for immediate needs. And except in the emergency room, decisions need not be made instantaneously. They have the time to go to the manual records or wait a few hours for a printout.

But the ease of programming in GALS and STARGEN does allow the system to respond to special emergencies. For example, when Rockland Psychiatric Center faced an employee strike, emergency plans had to be made to transfer 600 patients to other facilities. Each transfer facility received a computer list of patients and their drug regimes so that there would be no interruption in chemotherapy. This was done in one day, which would have been impossible without the computer.

Another emergency involved an ex-patient who was discovered to have amoebic dysentery. All the patients who had been in his ward would have to be examined for the disease, but many of them had moved elsewhere and historical lists of patient location are not kept manually. The computer retrieved a list of all patients who had been in that particular ward at that time plus their current locations. Examination of these patients revealed several more cases; they were treated, and a possible epidemic was averted.

At an MSIS facility in Connecticut, an ex-patient had allegedly committed a murder. When the press reported that he was a released patient, the Governor inquired whether the facility was releasing patients too soon. A statistical report was compiled on patient releases that showed the hospital was acting consistently with trends throughout the state.

The foregoing are only a few of the many examples of MSIS' versatility and capabilities. Now in its eighth year of operation, MSIS is a stable, proved system, which is attracting facilities all over the world to use MSIS forms and techniques in their own mental health information systems. In this country, facilities in Alabama, Nebraska, Hawaii and Tennessee use MSIS software, and the State of Tennessee processes the data for a Georgia facility. Overseas, Israel, Indonesia, Italy, Belgium and Canada--either governmentally or through individual facilities--now use MSIS forms and techniques.

In addition, there are several other advanced computer-based mental health information systems in operation, such as the Missouri Department of Mental Hygiene, the Walter Reed Army Medical Center in Washington, and the Fort Logan Health Center in Denver. There are also regional or national computer networks organized around identified records about a single disease or condition, such as the National Arthritis Data Base system created under the National Arthritis Act of 1974. There is no doubt that the techniques pioneered by MSIS and similar single-facility or multi-state information systems will be used far more widely for mental health and other medical data systems in the coming years. This gives the policies of MSIS as to citizen rights their special importance.

Citizen Rights Issues

Because MSIS is a pool of patient information drawn from many health-care centers in many states, and MSIS itself does not administer care or adjudicate payment claims, several elements of citizen rights discussed in other profiles are either peripheral to or take on different forms for MSIS.

Take the issue of patient access, for example. MSIS has never been asked by a patient to provide his/her record; if it were, it would refer the patient back to the facility where the treatment originates and the original record was generated. The patient access policies of the participating facilities run the gamut (very narrow) of similar mental health care facilities, whether the records are kept manually or computerized. Some require a court order from the patient's attorney to verify that the attorney is representing the patient and there is "good cause" to provide the record (advice of the Mental Health Officer at Rockland); others require a subpoena (Connecticut Mental Health Center), although this Center's clinicians are sometimes willing to discuss a patient's record with him without actual providing a copy of it. But in any case, MSIS does not set the standards for patient access to the original records kept in participating facilities, and it believes that patient access is "not an issue."

The Connecticut Center reports that "patients are asking to see their records now." In the spring of 1974, ABC television broadcast a program called "The Paper Prison," dealing with a variety of record keeping settings and detailing people's problems in getting access to and correcting their records in schools, police departments, the military, and delinquency programs. Following the program, the

Connecticut Mental Health Center has received about 8 or 9 requests per month from patients who want to see their records, compared to 1 or 2 requests per month previously. No one has specifically asked for computerized records. When a patient requests his records, officials at the Connecticut Center tell him that they cannot give him the records unless he obtains a subpoena or arranges this directly with his clinician. Many clinicians will share information from the records with the patients by reading it to them or discussing it with them, but very few doctors agree to show the records to the patient or provide a copy of them. According to Michael Levine of the Center, several patients have gone to court over access rights, but so far all of them have lost. He feels that eventually this situation will change, and when it does, the nature of the patient record will change; doctors will withhold certain information from the record if they know that the patient may read it.

As a theoretical matter, Dr. Laska states that MSIS would like to work with its user panels and with advisory groups to make the system "a pioneer in affording patient access." But it is not clear just what this would mean, and he recognizes that any system giving patients access to MSIS files themselves would probably require passage of new access laws in the participating states.

The issue of privacy in the MSIS system, in the sense of what patient information is collected and recorded, should be examined in light of the flexibility MSIS gives participating facilities in deciding what data to store in the MSIS computer. It is worth repeating in this context that only six of the 37 informational items on the Admissions form must be completed to open a patient record, and the only other form required is a Termination record. Moreover, participating facilities may omit the patient's name and social security number entirely, using a unique number or code as the record key. Beyond the minimum items, MSIS does not mandate what information is to be stored, or provide guidelines about what data collected locally is to be used only at that facility, whether manually or computerized. These practices vary from state to state and from one participating institution to another. For example, Massachusetts does not collect and store patient drug abuse information, and Connecticut does not store any information on patients' criminal records.

Some participating institutions provide chaplains with a list of inpatients of their faith, so they will know whom to visit. One facility gets a list of Jewish patients to whom matzoh will be distributed during Passover. Some participating states use ethnic and religious data to insure that there is no discrimination on the part of service delivery agencies. But again, what information is collected by the participating facility and for what purpose it is retrieved depends on decisions made by the facility, not by MSIS, and these decisions would likely be made the same way whether the records were kept manually or computerized, whether stored locally or centrally. So the issue of privacy, in the context of MSIS, is interesting, but not central.

What is central is the confidentiality of the records that MSIS stores. "The mere fact that a patient has been hospitalized in a psychiatric institution must be kept confidential," Dr. Laska believes. How to assure this is the direct responsibility of MSIS, and its managers have done considerable thinking- "agonizing" would not be too strong a term - about how to create an unbreachable system, - one that would be both legally protected and physically secure at each end so that the data flowing between the participating facility terminal and MSIS could not be intercepted.

In part, the MSIS efforts were stirred by public attacks on their operation. In May of 1970, an article appeared in the New York Times describing computer uses in the mental health field; one of the examples treated at length, in generally favorable terms, was MSIS. A month later, Jack Anderson wrote a nationally-syndicated column that attacked MSIS as a threat to patient privacy and the confidentiality of the physician-patient relationship.

"A New York State hospital," he said, "at a cost of millions to the taxpayer, is assembling an awesome data bank of highly specific, supposedly confidential information about psychiatric patients in seven states." MSIS "could be another step toward a national data center," which would "extinguish forever the right of privacy." Anderson was particularly concerned with the possibility that government investigative agencies could subpoena patient information and that the "all-knowing, never-forgetting electronic machines could produce at the press of a button a person's life from cradle to grave."

The Anderson attack was followed by inquiries from a number of concerned groups who voiced their concerns over possible violations of privacy. Senator Sam Ervin and a number of individual members of the House of Representatives wrote to HEW to find out what precautions were being taken to protect confidential information.

John Shattuck, the ACLU staff lawyer specializing in privacy issues, wrote also, and noted that the ACLU was particularly concerned that "without proper safeguards, these (psychiatric records) could well fall into the hands of unauthorized people."

In Sanford, Maine, employees of the state and federally funded York County Counseling Center refused to fill out the Admission and Termination forms, believing it an unwarranted invasion of privacy to amass and maintain such data on clients without their express consent.

To meet these problems, MSIS hired Dr. William J. Curran, Professor of Legal Medicine at Harvard, as its legal counsel in 1970. He and his staff surveyed the legal situation in each of the participating states and examined methods of insuring that adequate legal safeguards were present for the central databanks.

One possibility they considered was the transfer of control and ownership of MSIS to the New York State Department of Mental Hygiene; this would have brought into operation two sections of the New York State Mental Hygiene Law that protect confidentiality of department records. But since the records in MSIS concern patients in several states, it seemed inadvisable to place them under a government agency of another state. It was decided that the Research Foundation for Mental Hygiene, Inc. a neutral, non-governmental organization should retain control of the records, but that legal protection for the records at the Foundation should be secured.

One approach considered was the creation of an interstate compact, to be entered into by all cooperating states; this would establish the organizational framework of the system and guarantee the confidentiality of its records under rules that would be adopted by each state upon joining the compact. Such a compact was drafted by Dr. Curran, but a number of states rejected it as too formal for an operation at that time still regarded as in the experimental stage.

The alternative chosen was to seek a special enabling statute from the New York Legislature extending confidentiality to MSIS and all of its records. The statute would make the records private and privileged documents, not the property of the New York Department of Mental Hygiene, nor open to public-record access.

The bill, introduced into the New York General Assembly early in 1972, stipulated that the records and information stored in the system by facilities located outside New York were "not open for inspection by any agency or individual other than the agency or facility submitting (them)" and were "not subject to subpoena in any court or before any tribunal or administrative agency."

The prohibition of any subpoena was justified to the Legislature on the ground that all of these records are secondary sources of information and that the best evidence for any court proceedings is in the records maintained by the participating facility. Therefore, any subpoena should be addressed not to MSIS, but to the facility at which the records originated.

The bill also provided that the New York Commissioner of Mental Hygiene was empowered to conduct an annual review of the system to ensure its proper and lawful operation in the interests of the cooperating states and facilities. Finally, the bill gave MSIS the authority to release aggregate data for research purposes, provided that all patient identifiers were removed.

This path-breaking law to provide specialized status to a regional medical information system became part of the New York Civil Rights Law on May 15, 1972. Thus, the general confidentiality of records stored and controlled by MSIS were assured by law.

But it must be underscored that the confidentiality of records stored locally by the participating facilities (as with the questions of access and privacy) are still governed by the various state laws, just the same as other local facilities that are not participants in the MSIS system. In Connecticut, for example, a patient's record may be subpoenaed, and state laws require the mental health centers to give certain information to various third party payers. According to Lanse Crane, an attorney and assistant to the Director of the Connecticut Mental Health Center, the Welfare Department and the Department of Finance and Control have the widest access to patient information. "When it comes to issues of money and paying for treatment, confidentiality normally takes a back seat." MSIS sees the issue of bolstering the confidentiality laws in all their user states as an important task for their attention, especially as more states join MSIS or similar regional medical data banks. In late 1971, MSIS commissioned an analysis of the law in each of its participating jurisdictions. The study found that New York was the only one with a clear general statutory right of privacy. Court decisions in several other states recognized a common law right of privacy while two states, Rhode Island and Vermont, had not recognized the legal right of privacy.

As to psychiatric records specifically, the study found the New York law to have the broadest coverage here as well. New York recognizes a confidential relationship and creates a testimonial privilege for communications between patients and their physicians, psychologists, nurses and social workers. A few other states recognized only a patient-psychotherapist privilege.

As for patients' clinical records, consultant reports, psychological tests, drug administration records, and other records kept by mental health facilities, these are legally the property of the facility. Of the states that were then participating in MSIS (late 1971) five--Connecticut, Hawaii, Massachusetts, Vermont and New York--had statutes establishing the confidentiality of such patient records in mental health facilities. Neither Rhode Island nor the District of Columbia had explicit provisions protecting the confidentiality of such records.

MSIS has taken other steps with respect to confidentiality in addition to sponsoring the Amendment to the New York State Civil Liberties Law and to encouraging passage of state laws.

In 1973, Dr. Laska wrote HEW Secretary Casper Weinberger, requesting that MSIS be "authorized as a confidential system under Sec.45-82 of the Federal Public Health and Welfare Law." Such authorization would give MSIS the right to withhold information identifying the individuals who are the subjects of alcoholism research or treatment "from all persons not connected with the conduct of...research on, or treatment with respect to, alcohol abuse and alcoholism." Although the Secretary responded that a decision would be forthcoming quickly, as of late 1975, despite a second request, HEW had given only unofficial indications that MSIS would be covered. MSIS is assuming they are covered, but still awaits an official finding and notice.

Physical Security

Several technical safeguards are employed to protect the physical safety of MSIS records. Through a password system, each terminal has access only to its own data files, not those of any other user. Entrances to the Research Center where the MSIS computer is located are guarded by personnel or by electrical security devices. A guard is posted at the only entrance left open at night; all other entrances are locked and are protected by an alarm system. The computer room itself is locked with a combination lock at all times. At each of the participating facilities in which terminals are located responsibility for securing of the terminal room is in the hands of the director of the facility, and practices there vary from highly secure to fairly casual.

A good example of this involves patient notice of and consent to the MSIS operation. ACLU chapters in several of the states participating in MSIS have complained that while patients expect their records to be compiled and used in the local facilities treating them, or that identified data may be needed for state health-care evaluation and planning, they do not expect--nor would all of them welcome--the sending of their extensive, highly-sensitive records to a central computer in New York State. The ACLU complaints have stressed that MSIS may be an exemplary system in terms of its confidentiality safeguards, but, if so, it should be all the more willing to have the patients whose records will be lodged there informed of this practice. When the purposes and uses of MSIS and its protections are explained, the patient (or a legal guardian in case of incompetence) can make an informed decision as to whether his or her records should go into MSIS. Not to provide such a process, the ACLU groups charge, is to create just the kind of "secret data system" that the 1973 HEW Report, the federal Privacy Act of 1974, and several state fair information practices acts have condemned as unacceptable. MSIS officials have not yet faced this issue head on, but have treated it as a matter governed by the notice and consent policies of the local facilities.

Despite its efforts on behalf of confidentiality, and more important, despite the fact that no one has documented a single leak of information from MSIS in the eight years of its existence, or any violation of the strict rules of confidentiality under which it holds personal patient data, MSIS continues to draw considerable public fire on citizen rights questions.

Future Plans

MSIS personnel are developing a financial system to help mental health facilities track costs. Their major new activity currently is development of an information system for treating the mentally retarded, under a 3-year grant from the Social Rehabilitation Services of HEW. They are also conducting studies under an NIMH grant of how psychiatric records are actually used by clinicians and institutions in their decision-making as to treatment. Another project is to design an outpatient drug review system. MSIS officials see the use of their system as a bedrock for PSRO review of mental health care, and a necessity if and when a national health insurance program is enacted. "MSIS will have a major role in setting quality care standards in psychiatry," Dr. Laska believes. Meanwhile, new states continue to come onto the system each year, or utilize its software, or purchase its forms.

Observations

Considering all of MSIS efforts, and considering its unbreached security record, the protests about its activities, in another era, would very likely be considered somewhat paranoid. In today's world, they are, alas, all too plausible. In the last three years, the American people have been bombarded with documented accounts of government investigators illegally obtaining confidential information--confidential information protected by both physical security and by laws as stringent as the New York State Civil Rights Law. While the break-in at the office of Daniel Ellsberg's psychiatrist and the exposure of Sen. Thomas Eagleton's psychiatric history* are the most notable in the area of mental health records, other violations have done as much or more to create cynicism about the supposed confidentiality of health records. The FBI's illegal wire-tapping of members of the National Security Council, the CIA's illegal opening of mail of hundreds of thousands of American citizens; the stealing of records by the FBI or its informants belonging to anti-war groups such as the Institute for Policy Studies - all these and more have heightened public consciousness of the fragility of so-called confidential records. Adding to the climate of distrust are the activities of local law enforcement agencies which have been revealed in the past few years: police departments in most major American cities, New York, Baltimore, Washington, Chicago and Los Angeles among them, have been charged with illegal procurement of confidential documents.

In this atmosphere, it is easy to conjure up situations in which the confidentiality of systems like MSIS might be overridden in the interest of "national security"--tracking down a potential presidential assassin, say, or an unstable security risk. It is easy to imagine that its confidentiality might be overridden for law enforcement--tracing a kidnapper who was thought to be an ex-patient. Once breached for such overriding concerns, the system might be riddled by investigations of every kind because the very existence of easily-retrieved, identified records on people whose problems include drug abuse, alcoholism, sexual deviations and violent episodes is a tremendous temptation to local and national law enforcement agencies; therefore the very existence of such systems threatens citizens' rights, its critics conclude.

---

*Made public, ironically, by Jack Anderson.

There is no facile answer to the question of how to reconcile the need to deliver the improved mental health care that MSIS promises with the need to guarantee, in some as yet undefined way that goes beyond the laws and beyond physical security, the total confidentiality of mental health records. Yet the public acceptance of systems like MSIS will depend on developing strong and publicly-acceptable safeguards. Again, we will return to this issue in our concluding chapter.

SOURCES

A site visit was made to MSIS by Alan Westin and a visit to the Connecticut Mental Health Center, New York, by staff member Jamie Broder during the summer of 1974. Continuing contacts were had with MSIS officials by Alan Westin and Helene Toiv down to February of 1976.

The most detailed discussion of MSIS can be found in Eugene M. Laska and Rheta Bank, Safeguarding Psychiatric Privacy: Computer Systems and Their Uses (N.Y.: John Wiley and Sons, 1975). Other useful publications include: Eugene M. Laska, et al., "The Multi-State Information System," Evaluation, Fall, 1972, p.66 ; Jeffrey L. Crawford, Donald W. Morgan, and Daniel T. Gianturco, Progress in Mental Health Information Systems: Computer Applications (Cambridge, Massachusetts, Ballinger Publishing Company, 1974); IBM, "The Multi-State Information System for Psychiatric Patients," Application Brief; Eugene Laska, Ervin Varga, Joseph Wanderling, George Simpson, George W. Logemann and B.K. Shah, "Patterns of Psychotropic Drug Use for Schizophrenia," Diseases of the Nervous System, 34: 294-305, August/September, 1973; Carole Siegel, et al., "Evaluating the Attainment of Process Objectives of Community Mental Health Centers Using An Automated Patient Data System--MSIS," NIMH, 1974 ; William J. Curran, Eugene M. Laska, et al., "Protection of Privacy and Confidentiality," Science, November 23, 1973, p.799; Marguerite Zientara, "Mass. Crops Names on Multi-State Psychiatric Bank," Computerworld, November 7, 1973, p.4; Nancy Hicks, "Computer a 'Tool' in Mental Health," New York Times, May 3, 1970; Jack Anderson Column, in the Rockland, N.Y. Journal News, June 17, 1970; R. Clinton Taplin, "Computers--Mental Health Boon or Risk," The Record, May 14, 1973 (Hackensack, New Jersey).

For personal interviews, we are grateful to Dr. Eugene M. Laska; Rheta Bank; Dr. Boris Astrachan; Michael S. Levine; Lance Crane; and Robert Lawrence.

CHAPTER 10. MUTUAL OF OMAHA INSURANCE COMPANY

Mutual of Omaha is a multi-line insurance company with health insurance as one of its major offerings. A profit-making enterprise, its operations are guided by the standard of cost-effectiveness and commercial success. We chose Mutual because it is the largest and best-known of the commercial health insurers in the United States, because it is one of the most advanced computer users among Zone 2 service payers, and because recent privacy legislation has not only had some important effects on Mutual's data collection practices, but has also raised questions about how Mutual will select risks and administer claims investigations in the future.

Background on Mutual

Organized in 1909, Mutual has grown along with the health industry and is now the world's largest provider of individual and family health insurance. It offers policies covering hospital and surgical payments, extra hospital expenses, payments for specific diseases such as cancer, income protection for illness or hospitalization, and a variety of plans that take effect when programs like Medicare or Blue Cross stop paying. Mutual is licensed throughout the United States, Canada, Britain, Puerto Rico, and a few other locations. Seven other subsidiaries offer life insurance, mutual funds, travel insurance, and other lines, and Mutual's assets in 1974 were over $750 million.

Information Collection for Underwriting

As with other commercial insurance companies, Mutual, while eager to sell as many policies as possible, is also eager to weed out policy applicants who are poor health risks, or are unlikely to be able to pay their premiums, or might make fraudulent claims for benefits. These goals dictate the collection of a broad range of information directly from the applicant for a policy--information about the applicant's financial affairs, job and style of life, in addition to medical history. The medical part of the policy application calls for an account of injuries and medical treatment and a listing of diseases, including high blood pressure, arthritis, cancer, syphilis, epilepsy and mental disorders.

Until recently, Mutual's application included the question: "Are your and your dependents' morals and habits correct and temperate?" While few people were expected to answer "no", the company saw this as putting the applicant on notice that his/her morals would be considered in deciding to issue a policy. The question was recently deleted from Mutual's new application, after the company decided it didn't provide the underwriting department with any useful information. "What one person considers moral," comments Albert Hansen, Senior Vice President, "another does not...We are much better served by the specific inquiries (e.g. whether the applicant has ever been treated for alcoholism or drug addiction,or had venereal disease) in evaluating the individual medically as well as from those habits which could more likely affect insurability." The Company says that an admission of having been treated for either alcoholism or drug addiction will not by itself result in denying coverage, but would depend on the results of further investigation. In addition, "no" answers will not be investigated. However, should it subsequently be discovered (especially in a claims proceeding) that the applicant had not told the truth about a substantive matter, the insurance contract could be declared invalid and the claim denied.

Although questions about morals and habits are now omitted from the applicant's form, they still play a role when the company decides to make an investigatory check of the application. (See below).

In compliance with the federal Fair Credit Reporting Act, which took effect in 1971, the company includes in its policy applications a pre-investigation notice which reads as follows:

"This is to inform you that as part of our procedure for processing your application an investigative consumer report may be prepared whereby information is obtained through personal interviews with your neighbors, friends or others with whom you are acquainted. This inquiry includes information as to your or your dependents' (if family insurance) character, general reputation, personal characteristics and mode of living..."

This notice is detached from the policy and handed to the applicant when he fills out the form, to insure that proper notice has been given.

As part of the application, the prospective customer lists the doctors and hospitals from whom he has received treatment. He signs a statement which authorizes "any physician, hospital, insurer or other organizations having any records or knowledge concerning (the applicant) or (his) dependents to give such information to Mutual of Omaha Insurance Company." If important health history items are listed, the company, using this authorization, may check further with the physician or hospital. "In general, physicians and hospitals comply with our requests for medical data," remarked Hansen. "Of course, there is always someone who decides for one reason or another that everything is confidential." In that case, the company's medical personnel would evaluate the situation and decide whether to go ahead or to require further disclosure of verification from the applicant.

In addition to the individual application, Mutual uses a number of other sources to investigate some applicants. It checks its own files to see if there is any previous coverage or claims records. It has its own investigators make an inspection in cases where "an application is incomplete or otherwise suspicious, or because the policy applied for is a large one - for instance, to cover more than $300 per month in loss-of-time income."

Where their own investigators are not available, Mutual may get an "inspection report" from a commercial reporting firm such as Equifax (formerly Retail Credit) or Hooper Holmes.* Hansen notes that "these are fairly minimum checks; we get something on general character through reputation elicited from neighbors and references listed on the application - and we confirm things like employment, length of residence and neighborhood environment. We don't automatically assume that all of the information we see in an investigatory report is true. All findings are subject to verification." About a third of these investigations are done by Mutual's own people, and two-thirds by outside commercial firms. Of the 700,000 insurance applications received annually, about 50,000 (7%) are checked by investigations.

---

*Most of the reports that Equifax does for Mutual are Income Protection Reports, and are handled by personal or telephone interviews with the applicant. The report has sections on health, drinking, and drugs. Among the health questions are ones asking about any illnesses or operations, regular medication, rejection for military service or discharge for medical reasons, name and address of personal physician and "when was last visit, for what reason, what results." If the applicant is not available for direct interview, Equifax will contact an employer or neighbor and ask about that person's knowledge of these facts. Such persons are also asked whether they know "anything adverse about character, life style, general reputation or home environment."

Mutual approves at least 95% of the applications submitted to it. This means that about 30 to 35 thousand people a year are denied health insurance policies.

Health history is by far the most common reason for denying coverage, but other factors sometimes play a role. Actuarial studies which take into account age, sex and geographical area may also be determinative. "Sometimes geographical factors come up," a Mutual official said, "for instance in parts of some cities where the health and hospital facilities and environment may be very bad." Although it can be inferred that such geographical factors would be most likely to come into play in ghetto areas, whose populations are largely black or Spanish surnamed, race cannot be an explicit factor in insurance underwriting under federal Civil Rights Laws.

Asked about homosexuality in health insurance decisions, a factor about which protests have been raised in the life insurance industry, a Mutual official said: "It doesn't come up and we don't look for it; even if it did come up, we wouldn't use it unless there was accompanying information with some real health implications. You have to realize that we want to sell insurance and that most of our policy applications go through without a hitch."

Mutual, like most of the insurance industry, feels somewhat inhibited in its information-gathering activities because of the Fair Credit Reporting Act (FCRA). According to Hansen, certain applicants may believe that they no longer have to answer certain inquiries posed by investigators. As a result, the company finds that investigative reports that it purchases from outside commercial firms (Consumer Reporting Agencies, under the Act) are not as useful as they were before the FCRA was passed. "To illustrate, in order to qualify for insurance, a person must have a certain income. If an applicant's financial situation is shaky, for example he has walked away from two businesses and filed for bankruptcy, you may not want to take as great a risk on him as you might ordinarily, or you might want to charge a higher rate for the coverage applied for. For all we know, the applicant may be setting us up for a disability. The Fair Credit Reporting Act might preclude the company from securing that type of financial information."

Claims Investigations

Claims for benefits call for further information-gathering on policyowners. To collect on a claim, the policyowner must submit a proof of loss form on which he authorizes his physician to furnish medical information. Where a policy pays as soon as a disease is discovered, Mutual may request only a diagnosis from the physician. For other kinds of policies, detailed descriptions of medical procedures are required. However, the company says that most investigations of claims are made only to establish that the loss is covered within the framework of the policy provision.

Computerization At Mutual

In 1954, when Mutual's yearly business had grown to $5.1 million in policy applications and $5.9 million in benefit claims, a committee from Mutual and its life insurance affiliate, United of Omaha, began to plan for automating some of the firm's routine and costly high volume tasks. At every step in the planning process, Mutual officials recall, cost effectiveness was the key criterion. (A recent industry study found that Mutual's operational expenses are less than the combined average of the next 24 companies in the field).

James J. Kohanek, Vice-President for Computer Systems, says that since the company's first computer was delivered in 1957, the operation has grown so that "now we do everything but cut the lawn with our computers." The core of the system is its Consolidated Policy Accounting System, covering its regular lines of individual health policies and handling some $20 million in premium payments each month. This is a batch-processed file containing detailed records for each current policy: identifying information, premium payments, benefit information, etc. The system handles 70,000 benefit requests each month and issues nearly 9,000 benefit checks each weekday. On a given day, approximately 900,000 active benefit records are on tape, containing skeleton histories on the benefits granted and coded references to types of disability involved. The local Mutual representative, presented with a policyowner's benefit claim, can usually be supplied by the following morning, with the account information he needs to begin processing the claim.

Because Mutual finds benefit history important for developing new health insurance policies and for considering new applications from individuals already covered under another Mutual policy, they store on tape the benefit histories of more than 5 million policyowners. Each record contains items such as diagnoses, benefits paid, and actions taken on the policy. These are available on an overnight basis to authorized Home Office personnel.

In addition to active individual policies, the computer also handles the processing of benefits for its group insurance programs, keeps some records on Mutual employees and agents, and produces management reports.

Mutual's Role in Medicare and Champus Programs

Mutual serves as fiscal intermediary for Part B of the Medicare program (payment of doctor and outpatient bills) for the State of Nebraska, processing about 440,000 claims a year under an automated system developed by the Social Security Administration. It also handles 435,000 Medicare Part A claims (hospital bills) for various hospitals, health agencies, and nursing homes in 31 states and the District of Columbia; these are handled through manual procedures.

Eligibility data on all Medicare beneficiaries is stored in Baltimore in the computer files of the Social Security Administration. When Mutual receives a charge claim under Medicare Part B, it first conducts a computerized "medical audit" to see whether it falls within "acceptable parameters". A manual examination is done to see whether the treatment was really necessary and whether the health service rendered is covered by Medicare. Claims meeting these criteria are keypunched and sent to the SSA central file to verify eligibility. If the reply is satisfactory, Mutual's computer issues the checks. Both by law and contract, eligibility information obtained from SSA tapes and communications cannot be used for any other purpose.

According to Ben Patterson, Mutual's director of Medicare Administration, the automated system is by no means flawless. There are often delays in receiving eligibility data from the Social Security Administration, and each time there is a legislative change in the program, it takes a substantial period of time for the computer programming alterations to arrive from Baltimore. Nevertheless, "(i)f it weren't for the computer there would be no Medicare program," he said; "we would be drowned in data." Furthermore, the problems of detecting duplicate claims has been substantially alleviated.

The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) is a federal program, to pay the cost of civilian medical services for dependents of armed forces personnel where such services are not available in military hospitals. Eligibility is limited to dependent spouses and children of service members on active duty or training; certain retired service people, and dependents of service people killed on active duty. Among the services covered by CHAMPUS are treatment of medical or surgical conditions; nervous, mental and emotional disorders; chronic conditions and diseases; allied medical service such as occupational and physical therapists, audiologists, social workers, and remedial reading teachers; abortions, if locally legal; family planning services, marriage and pastoral counseling; and prescription drugs.

Mutual processes CHAMPUS hospital claims in seventeen states and physicians claims in six states plus Puerto Rico, Canada and Mexico. CHAMPUS claims are processed by an integrated on-line system, with sixty-three terminals.

Fifty-six terminals are dedicated to the claims audit function and each CHAMPUS claims auditor is issued a code that permits access to these terminals. When a claim is received, the claimant's name, social security number, date of birth, and other identifying data are fed into the computer, which audits the charge for the services rendered. In addition to issuing checks to claimants, the computer generates daily disposition lists of all claims processed, letters to claimants requesting additional data, and explanations of benefits.

Sixteen months of benefits history are stored in Mutual's CHAMPUS data bank. History data beyond that period are stored on microfilm. All claim records are filed in cabinets and are identified by an internally developed numbering scheme.

Originally, Mutual processed all CHAMPUS claims manually. The decision to automate in 1972 was prompted by the program's requirement that intermediaries develop fee profiles on physicians rendering health services to CHAMPUS beneficiaries.

Citizen Rights Issues

1. Confidentiality

Mutual regards its information about policyholders as confidential, for internal use. However, it faces many problems involving release of such data to outside agencies, and its sharing practices have undergone significant changes during the past few years. For example, health information is no longer shared within the industry through industrywide pools. Mutual used to forward limited information on policyowner's suspected of filing fraudulent claims to the Casualty Index, an industry file in New York which maintained national records for this purpose. The practice was discontinued in 1970. Mutual felt there was little danger to policyowners in contributing to and using the Index, but they were concerned about what policyowners might think about this exchange, and it was ended.

Where a group health policy is written for all the employees of a company or agency, and Mutual administers it directly, Mutual does not release identified employee health information to the employer. However, if the employer administers the program through its own claims office, Mutual has no way of knowing what is done with information about physical or mental conditions that might be disclosed in claims forms. Dr. Robert Long, Mutual's Associate Medical Director, noted that there might be extreme situations--"entirely theoretical so far"--in which Mutual might learn of a health condition and feel itself duty bound to notify the employer, such as "a person who was epileptic working with heavy machinery."

In 1973, in order to insure compliance with the Fair Credit Reporting Act, Mutual revised its regulations governing the release of information to other insurers. Without a signed authorization from the policyowner, release of information is now limited to the policyowner's name, address, date of birth, and occupation, plus the type of policy issued, issue date, amount of coverage, and the current status of the policy. With a signed authorization, release is limited to the previously described items, plus the amount of benefits, other final claims dispositions, and the source references of medical information contained in claims files up to the date of the authorization.

As far as state and federal agencies are concerned, Mutual officials give confidential data only when"we have no legal basis for denying the request." Mutual General Counsel Robert Muchemore recalled one instance in which the Missouri State Insurance Department insisted on copying various files. Mutual balked, but eventually complied when it realized that the Department could compel the production of these records at the Insurance Department, which could then make copies. The Internal Revenue Service also demands and obtains individual data from Mutual. By law, the IRS has a lien on monies due beneficiaries who are federal tax delinquents. As a result, Mutual is required to respond to IRS inquiries as to whether or not the company is liable to a particular policyowner. If so, Mutual must withhold the benefits from the insured and pay it over to IRS.

At one time, IRS requested health insurance carriers to report all payments made to policyowners in reimbursement of doctor bills. A number of companies vigorously resisted, and IRS backed down. However, as of 1971, all insurance companies must report to IRS the names of physicians to whom they have paid more than $600 a year.

Law enforcement officers occasionally approach Mutual with a fugitive warrant and ask for the address of an individual. This is provided. However, "no medical or benefits information is released," according to Mutual officials, and Hansen could recall no instance in which law enforcement agents requested such information.

"FBI agents come around perhaps three or four times a month," says Mutual official James Barrett. "Usually what they want is location information, or they are interested in the flight insurance area - for sabotage cases and for tracing the interstate movement of criminals."

In spite of the fact that some reporting to the federal government must be by social security number - (payments to physicians, Medicare and Champus claims) - Mutual continues to use its own numbering system for individual accounts. According to Kohanek, the company does not want to adopt social security numbering because it would "greatly increase the problem of confidentiality."

2. Computer Security

Officials at Mutual recognize that computerization leads to greater demands for both identified and statistical data. As an example, Mr. Kohanek mentioned the IRS requirement on reporting payments over $600 to physicians, and he commented: "The only reason we're asked to do it is because it can be done now by computers." Before computerization it would have been prohibitively costly to retrieve the requested data. Today, the government knows that the data are readily available at little cost, and so they demand it.

Protection of files from unauthorized access was included in Mutual's earliest computerization plans. Only authorized personnel are issued access codes to the computer, and only within their delegated area. For example, though the underwriting department is given access to information collected by the claims department, the claims department is not thought to require underwriting data and so claims personnel are not provided with underwriting access codes. Medicare and Champus personnel each have access only to their own data files.

All requests for information not covered by existing rules must be in writing and approved personally by Kohanek, a requirement that he feels has cut down the number of requests. The move to computers by itself reduced the number of people handling and duplicating files, and this, too, reduced opportunities for unauthorized access.

Physical security for the computer was strengthened in 1969 following a false bomb threat. Accounting controls over the huge sums of money involved in income premiums and outgoing benefits also operate to prevent unauthorized access. In sum, Mutual officials believe that confidentiality is fostered by their computer security rules and procedures.

The company stresses confidentiality to its agents and home office personnel. Training materials instruct them never to release confidential information to unauthorized people, never to translate the codes on rejected applications for anyone; and never to discuss confidential information with applicants, policyholders, or physicians. Every three or four months, Mutual distributes a bulletin reminding employees of the company's confidentiality rules. According to Hansen, Mutual has never had any problem with employees divulging confidential information. General Counsel Muchemore said the company had not received complaints of breaches of confidentiality, nor had it been sued over such an issue.

3. Policyholder Access

Policyowners are permitted to see their files (including data secured by inspection reports) so long as they furnish proper identification. The data is given only in person, and not over the telephone. However, policyowners will be given copies from their files only of statements they have signed (e.g. the application form) and the bills they have sent to the company for payment; other documents especially those from third parties, cannot be copied.

Mutual believes that insurance carriers should disclose medical information not known to the individual only to a personal physician, not the individual directly. "This will come closest to an absolute guarantee that such information will be properly explained," Dr. Long stated, and "the possibility of arousing feelings of doubt, fear, anxiety, or anger will be held to a minimum." Thus when Mutual gets medical information from a hospital or physician that affects its underwriting decision, and if the applicant asks to see this, Mutual will write back to the hospital or doctor and call on them to explain it to the patient. "We don't want to interfere with the doctor-patient relationship," said Dr. Long.

The Fair Credit Reporting Act has played a significant role in expanding consumer access to insurance company files, including Mutual's. As noted earlier, insurance companies must notify each applicant that the company may investigate or verify the personal information supplied. If insurance is denied on the basis of an inspection by a Consumer Reporting Agency (that is, one of the outside commercial firms as distinguished from Mutual's own investigating staff), the insurance company must give the applicant or policyowner the name of the company making the report, and he may then go there to find out its content and take further action if he thinks it is incorrect.

Gene Retz, second vice-president for underwriting and renewal, says that Mutual receives relatively few inquiries or complaints under this law - generally less than five a week. "To the best of my knowledge, we haven't needed to correct any action yet on the basis of anything turned up in a customer inquiry, though we'd be glad to if we found out that there had been some mistake."

"Many of the calls we've gotten," another Mutual official noted, "are the result of the notice people receive informing them that an inspection investigation will be completed. They want to know who we will ask, what the topics will be and so forth. We certainly don't have any difficulty replying to any of those calls."

For its work in Medicare, Mutual comes under the federal Privacy Act of 1974 (P.L. 93-579), which became operative in September of 1975. Regulations under the Act designate carriers and intermediaries under Medicare to be components of the Bureau of Health Insurance of the Social Security Administration. This requires them to:

(1) permit an individual to determine what records pertaining to him are collected, used, or disseminated by such agencies;

(2) permit an individual to prevent agency records pertaining to him from being used for any purpose not compatible with that for which obtained;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, and to correct such records when appropriate.

In order to comply with the requirements of the Privacy Act, each Medicare contractor must:

(1) inform each individual from whom information is requested of his or her rights under the Privacy Act;

(2) identify pertinent systems of records to be described in the Federal Register;

(3) describe the method of accessing individual's records;

(4) prepare a method of accounting for disclosures;

(5) devise a method of reviewing records at the request of individuals and making corrections if appropriate.

Mutual has instituted these procedures, but it is too early to judge what effects the Act will have on either Medicare claimant behavior or the underwriting and claims processes. When queried in March of 1976, Dr. Robert S. Long, Mutual's Associate Medical Director, reported that the company had received few if any Privacy Act inquiries under either Medicare or CHAMPUS. There was some concern at Mutual that the Act might cause reporting sources to "dry up" a bit, at least temporarily while the Act's provisions were being studied and experience under it observed.

Observations

Mutual's experiences as a highly-automated service payer indicate that computerization has not changed the way it deals with citizen rights. Its traditional policies protecting the confidentiality of policy-holder and beneficiary data have been reproduced in its automated systems. Data security is probably enhanced rather than lessened in its computerized systems. And as Congress has written new laws to protect citizen rights, Mutual has complied as fully in its automated as its manual operations, and as well as health insurers who are less computerized.

The important citizen rights issues that lie ahead for firms such as Mutual are almost entirely issues of social policy, not technology. Will American society choose to intervene by law in the risk-selection process to limit the criteria that may be used (and the investigations made) by insurance companies--as with sexual preference, cultural life style, and racially-based "objective" health conditions? Will society reject Mutual's stand in favor of revealing sensitive health data only to a chosen medical representative, rather than the individual directly?

For the first of these, the fact that Mutual is a private profit-making organization is important, since the selection of risks is critical to competitive success, and private firms have sometimes been allowed to continue applying criteria of selection that government--bound by the Bill of Rights--cannot. But in the second area--patient access--Mutual's position echoes that of most government health professionals and agencies, and it would be mistaken to apply a public-private distinction.

Beyond these questions lies the role that firms such as Mutual will play in any future system of national health insurance. The possibilities range from their being intermediaries in almost the same fashion as Mutual now is for Medicare and CHAMPUS to their role being limited to the offering of supplementary insurance beyond a basic, population-wide, government-administered health payment plan. Important citizen rights issues will be involved here, and we will return to this theme in the report's final chapter.

SOURCES

Part of this profile is drawn from an earlier site visit to Mutual and the resulting profile developed by the Project on Computer Databanks of the National Academy of Sciences' Computer Science and Engineering Board. This was published in Westin, Alan F. and Baker, Michael A., Databanks in a Free Society (New York: Quadrangle/The New York Times Book Company 1972) pages 143-154. A site visit for this project was made in August of 1974, by staff member Richard Silberberg. Thereafter, additional written materials, letters, and telephone interviews were developed through March 10, 1976, primarily by Helene Toiv and Alan Westin.

The following Mutual officials provided interviews used in the writing of this profile: Senior Executive Vice President Albert Hansen; Executive Vice President for Government Related Programs Charles Hermanek; Director of Medicare Administration Ben Patterson; Assistant Vice President for Medicare Administration Richard Bath; Assistant Vice President for CHAMPUS John Wrabetz; General Counsel Robert Muchemore; Associate Medical Director Kenneth Fletcher; Assistant Vice President Len Tondl; Associate Medical Director Robert Long; Mr. Thorne Dillon; Mr. James Barrett; Vice President for Computer Systems James J. Kohanek.

Part Four
Policy Alternatives

CHAPTER 11. ASSESSING THE COMPUTER'S IMPACT ON CITIZEN RIGHTS

The purpose of this chapter is to analyze the impact of health-data computerization on the citizen rights identified in Part One. At the outset, this requires consideration of the social setting in which such computerization has been proceeding. While we have touched on some of these themes before, in the survey of manual record-keeping and the profiles, it is important to pull these elements together here, for they represent the atmosphere within which specific incidents need to be understood.

THE SOCIAL SETTING OF HEALTH-DATA COMPUTERIZATION

The Computer Seen As An Instrument of Continuing Discrimination

The civil rights movement gave impetus to the formation of many groups of disadvantaged people struggling to overcome legal and social disabilities. In addition to blacks, other non-whites, women, and political dissidents, these groups include diverse sets of the population such as homosexuals, ex-mental patients, individuals in psychotherapy, people with arrest records, the physically handicapped, people with stigmatized diseases (epileptics, cerebral palsied, etc.), women who have had abortions, and ex drug or alcohol abusers.

The common element among such groups is their claim that they should have an equal competitive opportunity with others in the award of credit, employment, housing, education, licensing, and government benefits. They contend that using their special condition to block access to these opportunities represents a reliance on irrelevant or improper criteria.

On the whole, the trend in American law and public opinion during the past decade has been to accept the justice of many of these claims. Indeed, American society has already modified substantially the credential system that operated against such groups in the 1940's and 50's.

This development poses some sharp problems for organizational record-keeping. Once society has formally recognized a group's right to equal treatment, and sets up enforcement mechanisms to provide affirmative or even compensatory action, the recording of a condition is generally accepted as a practical necessity. Thus most women, blacks, and other racial or language minorities, whose conditions are usually obvious, do not raise an objection on the basis of privacy when organizations note and record their statuses.

For other disadvantaged groups, however, those who have not yet won full legal protection of their equality rights, preventing any systematic notation of their condition is a prime group objective. Sometimes, where their condition is not immediately noticeable, the objection is to organizations conducting intrusive personal investigations or forcing self-disclosure to identify these matters. Whether it is noticeable or not, these groups lodge a "privacy complaint" against the recording of this information because they know it will be used to restrict their rights and opportunities. The demand for privacy here is a tactic in the struggle to win social acceptance of their condition as immaterial to the decisions being made.

Groups challenging discriminatory data collection have as much concern with manual records as with computerized data systems that carry forward the existing standards. But they also see computerization as accelerating discrimination because computerized data systems usually involve more systematic collection, more extensive recording, more centralization, and easier dissemination. Health records have been a major area of such group protests not only when it is a purported "health condition" (being in therapy,etc.) that produces the social discrimination but also when the social data put into so many health records includes political, social, racial, sexual, or other criteria that are then used to make important "non-medical" judgments about people.

Growing Skepticism About "Data-Based" Government Social Programs

The profile of the Indian Health Service demonstrated the vital role that computers can play in collecting the data needed for planning socially useful programs. The computer records on the Papago Indians generated all sorts of statistical studies showing the relationship between poor housing and poor health; the role that poor nutrition played in certain diseases; what diseases were most prevalent; what special medical equipment was lacking, etc. But while the computer continues to turn out these studies, the housing of the Indians continues to deteriorate, the disease rate continues to climb, and their medical needs are not being met.

The gap between the health data collected by computers for socially useful programs and the actual delivery of such programs is commonplace, and it can affect peoples' views of the utility of data collection, as the following example illustrates. About ten years ago, private developers and the District of Columbia government undertook a slum clearance project for which they pledged the construction of enough low-cost housing so that the original residents of the neighborhood would not be displaced. As a first step, they initiated an elaborate study of the housing, transportation, schooling and medical needs of the residents, in which extensive personal information on welfare status, income, and health history was gathered and computerized to form a comprehensive picture of the neighborhood. In the end, however, only middle and upper middle class housing was built and virtually all the long time residents were displaced. With this background, the announcement in 1974 that the District government would renovate Kennedy stadium and as part of that renovation would replace the slums surrounding the stadium with low cost housing was greeted with some skepticism. When a comprehensive neighborhood study was initiated, local leaders urged the residents not to answer the questionnaires because, they said, the housing will never be built and the studies are just an excuse to collect personal information and that nobody knows how it will be used. In December, 1975, the city announced that while the renovation of the stadium would go forward, there were no funds available for the surrounding new housing.

The gulf between data collection and program fulfillment is especially striking in the federal government because, as an employer, it sets standards for private employers. Several years ago, the Department of Housing and Urban Development announced an affirmative action plan for increasing the number of its physically handicapped workers. It took a census of the number of physically handicapped at the agency and then set a recruitment schedule and final quota. While the plan was being implemented, the new HUD building was being built--being built without the ramps, electric eye doors, special parking facilities and other features that would make it possible for handicapped people to work them. Ultimately the protests of HUD employees, wide publicity, and the threat of a lawsuit forced HUD, reluctantly, belatedly, and at great expense, to install these special features.

These examples would belong only in a study of government planning and service-delivery were it not for the fact that large numbers of citizens are being asked in these programs to disclose personal information in order to help government make "rational" decisions. It should not be a surprise to government officials that when such "rational" enterprises fail to behave rationally--that is, to do what their announced objectives declare--citizens will become increasingly disbelieving of the promises under which they are being asked to reveal personal data.

General Distrust of Government and the Watergate Fallout

If we were living at a time of high citizen respect for government and social institutions, disbelief about government promises might be regarded as a minor issue. Government officials would generally be trusted not to misuse the sensitive personal data they had acquired, and the problem involved would be the costs of having collected and stored all that personal data without it being effectively used.

Trust in government, however, has never been a staple of the American political system. Based on the Founding Father's classically-grounded fears about inevitable misuse of government power, our system rested its faith on constitutional limits to government authority, public exposure of government's affairs, and Bill of Rights protections for individual and associational liberties.

The years from 1932 to 1968, broadly viewed, produced a great enlargement in the American public's acceptance of government authority. This grew out of well-known developments--the need to end the Great Depression, install major social programs to help the needy, wage the Second World War and then the Cold War, carry out the Great Society programs of the 60's, and provide affirmative support to the race and sex equality revolutions. Most conservatives accepted those parts of expanding government that supported business, defense, and overseas activity, while most liberals were enthusiastic about the new social programs, with each expressing reservations over the other's basis for supporting enlarged government roles.

However, since the late 1960's there has been a visibly growing public discontent with and distrust of government in the United States, a sentiment well documented by careful opinion surveys. Conservative critics have attacked centralized Big Government, urging a return of funds and decision-making to the state and local levels as well as using private rather than public programs wherever possible. Many liberals have become disillusioned with the failures of recent government programs to have fundamental effects on poverty, crime, bad education, drug rehabilitation, race inequitites, and similar problems. Within both ideological camps, the shortage of viable government programs has also led to doubts about using legal coercion to collect and store extensive personal information, especially from "client population" --senior citizens on Social Security and Medicare; welfare recipients; children; persons in drug rehabilitation programs, etc.

All of this might have still remained at "normal" levels of American distrust about government had it not been for Watergate and its successor revelations. The

Watergate disclosures of how top officials of the federal executive branch abused Internal Revenue Service records, conducted mail covers and openings, used illegal wiretapping and bugging, spied on political critics and dissident groups, and resorted to burglaries and break-ins came as a shock to the American public. All the "what if" warnings of civil libertarians about possible misuse of government powers suddenly became real rather than hypothetical situations. As several leaders in the psychiatric profession stated recently, "The break-in at Dr. Fielding's office to secure Daniel Ellsberg's psychiatric records was the last straw for us. From then on, we had to make protection of confidential records a top priority of our profession."

Revelations since the Watergate disclosures of 1973-74 have, if anything, deepened public concern over the security of personal data from misuse. During 1974-76, documentation of admittedly illegal or improper surveillance activities by the FBI, CIA, and IRS have convinced the average person that the label of "confidential" on any personal file held in government may be slender insurance against the efforts of federal, state or local investigators to get information, either overtly through the "buddy system" or by covert means.

Thus the call for personal data to carry out even the most laudatory government programs, managed by even the most socially-minded and confidentiality-oriented professionals, must bear the burden now of the Watergate and post-Watergate revelations. If this seems unfair to those government officials or proponents of social programs who were wholly outraged by Watergate, such are likely to be, for some time, the painful consequences when the highest elected and appointed officials in a nation are found to have betrayed the public trust.

Consumerism Enters the Health Care Field

Consumerism as a movement rests on two basic premises: that people have a right to be truthfully and fully informed about the products and services offered for sale to them, and that law should step in whenever commercial products or government activities present a danger to public health and safety. Consumerism has joined hands with the civil rights movement over denial of credit or other commercial services to racial minorities or women, and it has found common cause with civil liberties groups over protection of confidentiality and rights of access in areas such as credit reporting, customer bank records, and school and college files. Medical records have often been part of these consumer/citizen rights campaigns, as with provisions dealing with medical records in the Buckley Amendment of 1974, the federal Privacy Act of 1974 and parallel state fair information practices laws, and proposed amendments to add medical information in consumer reports to the coverage of the Fair Credit Reporting Act.

The most common meeting ground for consumerists and civil libertarians is the demand for individual access to records. Using medical records as an example, the interests are common when the issue is the right of a patient, when he or she insists upon it, to examine the primary medical record and to know about any other uses made of it. The consumer's demand to know in order to make an informed "buyer's" decision about the nature, quality, and consequences of health care matches the civil libertarian's insistence that access is vital to informed consent in the doctor-patient relationship and the securing of due process whenever an individual's secular rights or opportunities are determined through use of medical information.

The Uncertainty of Law

As we noted in Part One, legal rules until recently have not been very clear and detailed on the key issues of privacy, confidentiality, and individual access raised by the growing use of health data in American society. Until the early 1970's, case law centered primarily on issues of testimonial privilege, and provisions for patient access usually arose only when malpractice actions were involved. Many statutes stipulated that medical or health data collected under their auspices were "confidential" but most did not specify what that promise meant, especially in terms of controlling the release of identified records to third parties for quality-care review, research, for law enforcement, under subpoena, etc. There were virtually no statutes or court decisions setting limits as to what medical data could be collected, or regulating which health data were proper and improper to use for making governmental and social judgments.

This situation began to change in the mid-1970's. Federal confidentiality statutes governing alcohol and drug abuse programs provided some detailed protections. The federal Privacy Act of 1974 and its counterpart in five states as of early 1976 provided important rules as to collection, use, and individual access to personal data in the hands of government agencies providing direct health care, conducting health research, or using health data to make evaluative decisions for employment, licensing, etc. Similarly, HEW's regulations governing confidentiality and access in the new federal PSRO system were more explicit and protective than anything in earlier federal review procedures.

Several things should be noted about this situation. First, many of the reactions to computerization of health data that we encountered and will analyze in this chapter took place before such new privacy laws had been enacted; they arose under the then-correct assumption by critics that there was no existing legislation to protect individual rights in the operations of such data systems. A second point is that the laws just mentioned are still new (the federal Privacy Act did not go into effect until September of 1975) and their effects are still uncertain; this is all the more true for the health field because these acts do not contain specific sections written to deal with the special problems of medical and health records. Finally, the entire private sector and 45 of the states are not covered by general privacy legislation, leaving quite a gap in the structure of citizen protection.

Thus the first major encounters by health professionals and citizen rights groups with computerizing health-data systems arose either before basic legal rights of patients and data subjects had been spelled out, or at a time when coverage of these acts for patient rights is still far from clear. As a result, various groups concerned over citizens rights have remained distinctly uneasy about accepting computerization of sensitive health data before rules and safeguards are fully installed.

Popular Perceptions of "The Computer"

When computers began to be used extensively in the mid-1960's to automate personal data files, much of the American public was fundamentally ignorant of what computers did and how. As a result of over-inflated claims of capability by computer enthusiasts and over-credulous acceptance of these predictions by persons worried about citizen rights, much of the debate over "computers and privacy" in the late 1960's was based on faulty assumptions as to the computer's real impact on data handling and decision-making.

This condition was rectified by the report of the National Academy of Sciences' Project on Computer Databanks in 1972. The NAS study, to which we have already referred, explained and corrected several popular misconceptions about computers. It showed that computer use did not automatically lead organizations to collect more intrusive information than they had collected manually; or to exchange data with different organizations than had been traditional, just because each had computers; or to be more secretive and provide fewer notice and access rights than the same organization did before it computerized. The NAS Report also showed that computers always respond to the explicit instructions of their owners as to how long to store any piece of information, what significance to place on any item, or what factors to aggregate in making a judgment about any person. In short, computers were shown to follow the policy directions of human owners and programmers as set by organizational managers or by law; they are not the "unforgiving, unforgetting" automatons presented by much of the anti-computer literature of the 1960's.

The NAS Report and other objective studies led most citizen groups, professional organizations, and political leaders in the mid-1970's to focus on the real citizen rights issues in record-keeping: whatever the medium of information storage and processing, what are the standards and procedures being adopted by organizational managers to make judgments about people? Opinion studies also showed that a majority of the public had acquired sensible judgments about many key issues of computerization, for example, that most of the goofs and rigidities of computer operations are the result of insensitive human actions, which can be remedied at acceptable costs if the public refuses to accept such performances. Passage of the Fair Credit Billing Act of 1975 is an example of the public's determination that computer systems should be made responsive to people, and not vice versa.

The importance of this for our purposes is that extensive computer use in health care arrived in the 1970's, after citizen rights groups, the media, and legislators had begun to acquire more sophisticated and accurate views of what computers can and cannot do. It also came after the public had shown that it accepted the "privacy campaign" as a legitimate and important area for regulatory action.

* * *

Other forces and trends might be mentioned in describing the complex social setting in which health computerization is taking place, and we have not tried to assemble here a comprehensive account. Our goal has been to note these developments that bear directly on citizens rights claims, and on that score, we think the major points have been made. Computerization of health data is unfolding in an atmosphere of considerable public mistrust over the motives, promises, practices, and performance of government agencies, mixed with a rapidly growing consumerist approach to health care and growing public belief that privacy protections should be instituted by positive regulation before sensitive new data systems are implemented.

ANALYZING THE COMPUTER'S IMPACT

Given the social setting that we have described, how can we analyze the impact that health-data computerization has had thus far on citizen rights? One important observation to start with is that instances of harm done to individuals--violations of confidentiality, refusals of access, etc.--are still almost entirely centered today on manual rather than computerized files. This is because manual files are the places where most of our detailed medical and health records are still being kept. Furthermore, even when some patient records are automated by Zone I providers, there is usually manual-record backup, photocopies, or computer printout floating around somewhere in the organization, and this remains an easier target for attack, as by reporters trying to get information on celebrities in hospitals, than are the computer files. Where record systems have been heavily computerized, as in the service payer organizations in Zone II, the complaints that we noted have also arisen primarily from employees of payer organizations writing doctors and hospitals to provide more detailed (manual) information than the providers thought necessary and proper, or when leaks of patient data were made in manual reports to employers about their employees' health conditions. Similarly, most of the disputed social judgments about people being made by organizations in Zone III, on the basis of health data, are also still based today on manual records.

Secondly, as we examined automation of health data in Zones I and II, we noted that records in their computer files are generally more subject to rules of restricted access than paper records located elsewhere in that institution or in similar non-automated facilities. Partly, this is because protection of the computer, its programs, and its continuous operations leads to stricter rules than are usually followed at nursing stations, record rooms, etc.; in this sense, privacy and confidentiality are serendipitous beneficiaries of computer security practices. However, we also noted that many of the computer professionals and medical or health colleagues who lead computerization projects in the health field are sensitive to the civil liberties issues, since these have been so widely debated in the computer press over the past half dozen years. In addition, a set of general systems techniques for controlling authorizations and access, maintaining audit trails, and taking protective measures over personal or proprietary data have been evolved and well publicized in the past few years, and these have been installed in many of the systems that we visited or studied. Thus, making a gross comparison as to the degree of protection given to confidential patient data in most highly automated systems compared to most comparable manual facilities, our judgment would be that the automated facilities are better protected today than most manual records against the kind of leakages and misuses that have been problems in recent decades.

What we conclude is that the main problem today in computerized health data systems is potential harm. As we will see, what makes such potential harm particularly serious for civil liberties is the fact that these possibilities of misuse have not been taken into account and dealt with effectively by the managers of such computerized systems.

To develop this analysis, we will present a series of incidents, collected during the two years of this project, involving the creation or use of computerized records. We will relate what happened, sometimes grouping several situations together, then offer comments on what the incidents suggest about computerization and citizen rights.

Incident: The Missouri State Division of Health[1]

In June of 1974, the State of Missouri's Division of Health ordered all Missouri hospitals, private as well as public, to provide abstracts of patient discharge data so that state health officials could "study the prevalence and control of disease in Missouri." The abstracts were to include: an abstract number; hospital number; medical record number; year and date of birth; admission data; discharge date; sex; race, color, or origin; marital status; residence (by census tract, zip code and street name); discharge service; expected primary source of payment; attending physician; discharge status; diagnosis; and surgical and diagnostic procedures used. Providing the patient's name was "optional" for the hospital. Failure to provide the abstract could lead to loss of the hospital's license to operate.

The availability of computers was officially cited as the reason for launching the mandatory data system in 1974. Garland Land, director of the Missouri Center for Health Statistics, explained that "the program has actually been in effect since 1963 on a voluntary basis. When the program was computerized to make it more efficient, 100 per cent of the data was necessary and its release was made mandatory." In addition to helping in the study and control of disease, state authorities said the information was vitally needed for better health planning and to avoid the construction of unnecessary or duplicative hospital facilities.

These explanations, and the way the new system was to operate, did not convince everyone in Missouri. St. Mary's Hospital in Richmond Heights, Missouri, announced that it would refuse to supply the discharge data. Patient authorization is required for all information released, St. Mary's said, and government agencies can be given only aggregate data in the form of statistics. Robert Thebeau, assistant executive director of St. Mary's explained that while the stated objectives of the state program "sound good," the way the state went about these is "not sound." All the state needs is statistical data, he declared, "but they want information about each patient."

Director Land replied that statistical data "isn't refined enough and presents limitations. Individualized data are needed because they are more easily analyzed. But this doesn't mean the data have to be personally identifiable. We don't ask for patients' names." State officials also noted that the June 1974 directive made provision for protecting patient privacy. A clause in the collection order stated:

"Any contemplated dissemination by the Missouri Division of Health of the data originally procured from a hospital and which contains evidence which might identify any individual person, hospital or physician can be carried out only with written permission of the hospital."

These assurances still did not satisfy officials of the Sisters of St. Mary's. Rosalie Merz, medical records administrator, said that once patient information is given to the state "there is no way we know it can be secure. There is no foolproof data processing storage system." Mr. Thebeau added that Missouri's "Sunshine Law" opens all state information not expressly exempted to public access, and there was no assurance that these records were exempt.

To deal with the threat they saw posed by the state data system, St. Mary's officials helped form the Eastern Missouri Task Force for Health Data Security, a group composed of hospital executives, medical record administrators, physicians, nurses, computer programmers, and systems analysts working in the hospital field. In its communication with the state health division, the Task Force stressed that it "does not question the need for comparable health data." However, "as a matter of professional ethics," Task Force members said, "we cannot submit clinical data to this data bank, or any other data bank, until we have been assured that adequate safeguards have been built into the system." In addition to asking that protective rules be spelled out dealing with confidentiality and data security in the proposed system, the Task Force suggested that such data ought to be maintained in special Ethical Data Centers, a new set of institutions operating under formal codes of professional conduct, "with explicit and appropriate operational standards, with clearly defined data access policies, and with stringent and continuing data security measures to ensure medical confidentiality." (The Ethical Data Center concept has been pioneered by Dr. Elmer Gabrieli of the E.J. Meyer Hospital, Buffalo, New York.)

By June of 1974, leaders of the St. Louis County Medical Society had joined in the opposition to the state's data plan. The Society's "Legislative Column," written by Dr. Edwin J. Cunningham, noted that the items of patient identification to be collected, even though they did not include name, would be enough to make identification of individuals "a simple matter." "In addition, the attending physician would have an identifiable number that would easily identify him and gain access to confidential information." Dr. Cunningham went on to report:

> The Ad Hoc Committee of the County Society regarding PSRO discussed this proposal in detail with several other guests recently. It was the feeling of the committee that since the need for this information and the authority to acquire it has not been clearly established, that we oppose such a proposal at this point. In addition, the utilization, distribution, and access to this confidential information is also unclear which poses a severe threat to confidentiality....
>
> Any legitimate data requested by the Missouri State Health Department can be met by currently operative mechanisms that insure that confidentiality is preserved.

In addition, Dr. Robert Deitchman wrote a scathing attack in the Medical Society Bulletin calling on doctors to rally the public against the state's proposal:

> Confidentiality--one of the keystones to the patient-doctor relationship will become a hollow word--a farce--if the state health organization continues with its on-going plans to computerize all discharge information from the hospitals....

> Despite crude and sparse material requested, a person with some knowledge can sift through the computer, checking out a specific person, pinning him down by age, address, date or discharge, and census block, to pinpoint any individual they see--and use it as they wish--regardless of today's promise it will all be done in desire for research and statistics....
>
> For the doctor this is a real threat to his oath as a doctor--but the public--they need to be warned, alerted, awakened to the silent death of their privacy amid the slowly turning hum of the computer and bureaucracy.

As opposition mounted, the Task Force directed another attack on the failure of the state health division to involve the medical profession, the bar, and computer experts before it ordered the project to proceed.

In November of 1974, the Attorney General of Missouri was asked to rule on the legality of the state division order. Before he could do so, however, the state health division announced in December of 1974 that it had reconsidered its order. The provision of discharge abstracts, it said, "will continue to be voluntary."

Comment

This episode contains several different elements typical of those that arise along with computerization: (1) the change from voluntary to mandatory compliance was dictated because the computer made processing of the information possible; (2) the need for the computerization of identified patient data for the purpose of hospital planning, evaluation and utilization review was not balanced convincingly against the rights of confidentiality of the patients; critics pointed out that the same socially useful goals could be carried out with unidentified statistical data; (3) the proposal to computerize identified data was not accompanied by any plan, draft legislation, or regulation to prevent dissemination of identified data; a mere pledge that dissemination of patient information would require permission of the hospital raised more questions than it answered, and no attempt was made to secure legal protection of the records from the operations of Missouri's public information; (4) special concerns were raised because of the possibility that once the data was in the state health divisions' computer files, it might be sought by other state health or welfare agencies with automated systems, or be demanded by federal officials administering federal health programs.

Several markedly similar incidents have occurred in other states; we will look at three together.

Incident: The Michigan Department of Mental Health[2]

In the fall of 1972, Dr. E. Gordon Yudashkin, Director of the Michigan Department of Mental Health, announced that a detailed "face sheet" report would be required on all persons being treated by local mental health agencies as a condition of continued state funding of their activities. These would go into a state computer file, where they would be used, Dr. Yudashkin stated, "to evaluate whether the poor and the really sick are being helped" and to facilitate the treatment of more people outside institutions. Opposition to the compulsory reports was immediately voiced by mental health agencies and the state ACLU chapter. A lawsuit in state court to enjoin the program was filed by the Michigan Society for Mental Health and the Shiawassee Community Health Board, alleging that disclosure of extensive personal and diagnostic information, stored by name, violated doctor-patient confidentiality and improperly invaded the patient's privacy.

Dr. Yudashkin replied that "the new system gives more privacy than the old one," under which Michigan's 50 state clinics had kept records by patient name for over 30 years. Under the plan to computerize data from the county mental health group, a "name code" is used based on every other letter of the name, and this protects confidentiality.

The complaining groups were not convinced that requiring the name was necessary for the state's evaluative needs, or that using the code procedure was a sufficient safeguard.

The initial court decision upheld the state, but while an appeal was being prepared, Dr. Yudashkin announced that the state could do its work well enough without names being furnished with face sheets and that he was rescinding the requirement for furnishing names.

Incident: The Washington Department of Social and Health Services.[3]

In the state of Washington in 1972, the ACLU had prepared the papers for a lawsuit against the King County (Seattle) Community Mental Health Service, to enjoin its director from furnishing the state's Department of Social and Health Services with identified patient case information. The state had ordered that this information be furnished by all private and community institutions receiving state or federal funds through the county mental health service. The plan was to create a central computer file in the state capitol, as part of the Department's Community Mental Health Information System.

The data that was to be furnished included identification information (social security number, birthdate, sex, marital status, ethnic origin, monthly family income, etc.); the diagnosis (by the American Psychiatric Association's diagnosis code); the type of activity used as therapy or treatment; who referred the person or group there; an evaluation of the problems the individual has with respect to job, school, home, family, thought process, emotion, marital, drug, or alcohol; and an identification by name and discipline of who made the diagnosis and evaluation. An additional report was to be required for each further contact with the center or agency after the initial report.

The ACLU suit against the plan was brought by two psychiatrists working on a contract basis with local mental health centers and by the director of the Jewish Family and Child Service, alleging that compliance would require them to violate the rights to privacy and medical confidentiality of their patients. The suit called on the state to "devise a data system where records cannot be ascribed to individual patients."

Before the suit was filed, an agreement was worked out with the state Attorney General providing that more limited statistical data, and without personal identifiers, would be all that local agencies had to submit to the state.

Incident: The New York State Department of Mental Hygiene[4]

No such negotiated settlement has been reached in a case currently being litigated in New York. In November of 1973, the state Department of Mental Hygiene promulgated a reporting form (known as the "MS-5") to be completed on each psychiatric outpatient by mental health institutions and sent to Albany, where its contents would be placed in the Department's computer system. The MS-5 includes the patient's name, social security number, extensive personal information, problem appraisal, problem severity rating, and other sensitive data. These include: "social relations disturbance," "social performance disturbance," and a list of 24 "other signs and symptoms" such as "suicidal thoughts," "grandiosity," "sexual problems," "anti-social attitudes," "narcotics," and "delusions."

The Mental Health Law Project was approached in late 1973 by several doctors and patients at the Tremont Crisis Center of Bronx Hospital, New York City, who objected to such identified forms being sent to the State Commissioner of Mental Hygiene and computerized in a state file. A lawsuit was filed on behalf of three doctors at the Center, three patients, and a social worker.

The suit alleges that the data-collection is "anti-therapeutic" since it would, when patients learn about it, deter some prospective patients from seeking treatment at the Center or lead present patients not to disclose sensitive information fully, thereby interfering with the professional activities of doctors and social workers. The suit states that the disclosures are in violation of the doctor-patient and social worker-client privileges of New York law; provisions of the state Mental Hygiene Law ("Names of patients treated at outpatient or non-residential facilities and at general hospitals shall not be required."); and of the patient's "constitutional rights to privacy, due process, and equal protection of the law."

The suit also challenged the degree of confidentiality that the data would have:

> The degree to which the information is kept confidential by the Department of Mental Hygiene is open to question. There is some indication that any doctor or employee of any state facility can obtain the information on any patient in the state simply by dialing a specific telephone number and requesting the information. By law the information is available to any court of record, the Mental Health Information Service (the legal advocacy system in New York), anyone receiving the consent of the Commissioner and of the patient, and with the sole consent of the Commissioner to any agencies which make payments on behalf of the patients, such as Medicare or Medicaid, missing persons agencies, criminal agencies, and the Firearms Control Board of the City of New York.

The suit asked that the MS-5 form be held illegal, or if that were not accepted, that patient data be kept only by number in the central computer and the links between number and patient name be kept only by the local facility.

However, the lower court upheld the Commissioner at the initial hearing, dismissing the suit on the grounds that the MS-5 represented a reasonable exercise of the State's powers. An appeal is now pending.

Comment

The three episodes above are similar to the first one (Missouri) in their basic outlines: the arrival of a computer stimulating the collection of such data; the lack of a demonstrated need for identified data for evaluative purposes; and the lack of accompanying legislation or regulations to safeguard identified data. The variations occur in the amount of detail required. Both the Washington and New York reporting forms go far beyond the identification-payer-diagnosis type of information requested by the first two agencies; they require submission of the most sensitive data about each patient. Even if a need could be demonstrated for the collection of some identified patient data for evaluative purposes, therefore, questions would still be raised as to how much and what kinds of data ought to be collected for such purposes. In addition, the law suit brought against the MS-5 form in New York focuses on the lack of confidentiality of the material, pointing out that by law the information would be available to courts, to service payers, to missing persons bureaus, and law enforcement agencies.

It is also worth noting that in three of the four episodes, the organized protests of professional groups or civil liberties organizations resulted in the projects either being abandoned or modified to take at least some of the citizens rights demands into account. The episodes also illustrate the tendency of many government agencies to plan and implement new automated data systems without providing notice to the population to be affected, professional groups, citizens' organizations, or to the public at large. Even where formal notices may be issued, there is often a practice not to hold meaningful consultations with interested groups or public hearings in advance of instituting such systems.

An example of this was reported in January of 1976 by Alan Taylor, a columnist for *Computerworld* who writes often about problems of making computer systems responsive to the people they are created to serve. Taylor related that the State of Maryland's Health Services Cost Review Commission published a brief notice in December of 1975 in the obscure *Maryland Register* announcing that it would require all hospitals to furnish each patient's Social Security number, the number of his/her "legally responsible" doctor or surgeon, and a list of detailed items of medical information.[5] The hospitals affected received no explanations, nor were patients informed of what would be done with the data. No public hearings were scheduled to discuss the reporting system, which was to go into effect in April of 1976. At a meeting in January,1976 of the Baltimore and Washington, D.C. Data Processing Medical Users Group, it was found that computer specialists in Maryland hospitals were unaware of the plan. By calling the Commission, Taylor was able to learn that the Commission intended to send the material to the U.S. National Institutes of Health, but little else was communicated. Taylor deplored this style of creating data banks with highly sensitive personal information, and urged that the Maryland Commission "delay its data base implementation until information is released and reviewed by an impartial authority and by the public."

Incident: The California Community Services Division[6]

In an effort to reduce costs and control eligibility standards for welfare recipients, the state of California computerized its welfare rolls and required local welfare offices to submit detailed reports on each client. The data to be furnished included reports as to the unemployability of individuals due to mental disability or the presence of mental illness, alcoholism, drug or narcotic dependency, sex offender status, mental retardation, unwed mother, unwed pregnancy, "mentally incapable of personal money management," and other conditions--some medical and some non-medical.

In 1969, two psychiatric social workers assigned to the San Francisco office of the state Community Service Division refused to comply with the requirement to submit these reports.

They maintained that furnishing such data on their clients to the state, for use in a computer system open to many unknown uses, would breach the confidentiality of the social worker-client relationship, their professional code of ethics to keep such information confidential, and the privacy rights of their clients. The State rejected the social workers' protest, and ordered them suspended and their pay forfeited for five days for "willful disobedience" of Department orders. The Northern California ACLU defended the two social workers in an appeal from this action, contending that the state welfare department's computer system was insufficiently secure in its confidentiality and security protections, thus justifying the social workers' refusal to submit the sensitive psychiatric and emotional data on their clients.

This position was rejected by the California courts at the trial and appellate court levels. A 1974 Appelate Court opinion held that the social workers had no psychiatrist's privilege under California law; that welfare client data is open to administrators of the welfare system; that collection of case data is essential to administration of the welfare program; that welfare clients are not entitled to notice nor is their consent required for inclusion of all their data in such a state computer system; that it was the Department's responsibility to see that the confidentiality provisions of the state welfare code were met in their management of the computerized system; and therefore that no right of privacy of the clients or privilege of the caseworkers had been violated. The five-day suspensions were thereby upheld.[7]

Incident: The Washington State Department of Social and Health Services[8]

In January of 1976, 200 caseworkers in the Washington State Department of Social and Health Services filed grievances protesting an order to supply the Department's computerized reporting system with extensive personal information on welfare clients. The state said these client reports were compulsory under Title 20 of the Social Security Act, as amended in 1975, which provides funds for the state's welfare system. The state welfare workers said that the new forms called for information in excess of what the federal law requires; that providing the information (which included physical and mental health data) would violate the confidentiality of the caseworker-client relationship; that the data coding required by the form produced "de-humanizing" categorization of individual situations; and that there were insufficient controls over the uses that would be made of the personal information and who would have access to it once it left the welfare agency's own files.

The state welfare department rejected the positions of the protesting case workers, and one woman with 15 years in the agency was fired for refusing to submit her client's data. The case workers who filed the grievances have been supported by their union, the American Federation of State, County, and Municipal Employees, and a lawsuit to block the reporting requirements has been threatened, with local civil liberties support, if the state does not modify its requirement.

Comment.

The common element here with the episodes described earlier is the concern over leakage of sensitive data to other government agencies, or over insecurely protected data systems. But the main purpose of California's computerization of welfare records is different from the computerization in the previous examples and raises another difficult question. In the previous examples, a compelling case could be made that identified data was not necessary to do program evaluation and utilization studies. But where the goal is welfare eligibility, identified data is obviously essential. If one accepts the proposition that the government has the right to impose and enforce welfare eligibility standards--a proposition that neither society nor the law seriously questions--then the issue becomes not whether or not to collect identified data, but how much and under what circumstances. Thus, the courts have ruled that in determining welfare eligibility the state may legitimately inquire as to how many members are in an applicant family and what their incomes are. However, the state may not conduct surprise nighttime visits to an applicant family to discover whether there is an "unauthorized" man living in the house (who might be supplying unreported income), since such visits violate constitutional rights to privacy.

Thus, the questions raised by the California incident are: (a) What limits should be set to assure that the information requested is relevant to the stated purpose in this case, welfare eligibility?; (b) Should these limits bar the collection of sensitive psychiatric and emotional data, especially in view of the fact that such data might be made available to other state agencies, especially law enforcement officials?; (c) Do clients have the right to know that information confided to a social worker will be forwarded to a central computer, and possibly be made available to other state agencies?

Problem: Juvenile Records

Juvenile records kept by both police departments and juvenile courts raise special problems because of the anomalous position of juveniles in our criminal justice system. Both the police and the courts assume responsibility for juveniles in cases where no criminal behavior is suspected or charged--runaways, truants, neglected children, psychologically troubled children, etc. Many states and large metropolitan areas keep extensive computerized records on such children, which includes educational, medical, and family background information. Moreover, many juveniles run afoul of the law, and are even taken into custody for behavior which in an adult would not be considered an offense. In New York City, for example, the Police Department maintains a computerized file for almost every minor who encounters the police (about 60,000 a year), and files a YD (Youth Division) card for each. A study conducted by the city's Criminal Justice Coordinating Council concluded that nearly half of the YD cards were filed for such acts as "loudness, boisterousness...use of obscene language, annoying people, throwing objects... swimming, etc..." In approximately 40% of these cases, the study found, there is no check on the validity of the initial decision to classify the behavior as an offense. YD cards are filed for the victims of offenses, although there is no evidence of improper behavior on the part of the victims. When a youth is innocently involved, or when the initial issuance of a YD card is unauthorized, the offense report remains in the data banks.

Despite such shortcomings, the study found the YD record to be a major determinant in the disposition of subsequent charges. Minors with three or four entries on their YD cards were much less likely to qualify for probation or to have their cases dismissed than those with no record, no matter what the seriousness or relevance of the particular entry. Length, not content, appeared to matter most.

A number of states have computerized juvenile court files, and the materials submitted to them are taken from the forms used by counselors who interview juveniles in connection with juvenile court proceedings. The ACLU has raised two questions about these forms.[9] First, the boxes to be checked include such terms as "schizoid," "Latently psychotic," and similar brief descriptions. "Instead of a complex diagnosis which any one of these conditions would merit," the ACLU project on Privacy and Data Collection recently noted, "the diagnosis is reduced to one word so that it can be easily computerized." The second concern is that the terms call for professional diagnoses, but the counselors are not medical doctors or psychiatrists. The ACLU goes on to state that though the juvenile or his/her representative may not see these labels, they are accessible not only to juvenile court personnel, but also "researchers, the FBI, the military and prospective employers..."

Comment

Previous episodes have raised the question of the need for identified patient information to be collected at all, and where the need for identified information is demonstrated, the amount of data that should appropriately be collected. That question is raised in a most striking way by the New York YD system (and many other metropolitan police juvenile division practices) because the collection of this non-criminal information, much of it containing sensitive psychological data, can lead to criminal penalties.

The question raised by computerized court records is the form in which the data may be collected; that is, does the short hand term fostered by computer coding distort the diagnosis, even if it is an accurate one? Should such diagnoses be used when made by a non-professional?

These questions are of particular importance because of society's policy towards juveniles. For these children whose "offenses" do not lead to court action, but are kept on police indexes such as the New York YD index, there is no protection against their records being exchanged with other police departments or private employers. In describing the Orange County, California Central Juvenile Index lawyers who defend juveniles say "The Central Juvenile Index is like a sieve. Every department store and every insurance company hires moonlighting cops and excops... because they or their buddies have access to the records..."

On the other hand, disclosure and recording of sensitive juvenile court records[10] is encouraged because of the widespread belief that juvenile records are either expunged or permanently sealed after a period of years, and therefore that the information in them will not be available to other government agencies or private organizations. Indeed, both the federal Youthful Offender Act and most state juvenile laws provide for this. But in fact, when juvenile arrests and/or convictions are reported to the FBI, they are not specially sequestered, but are placed in the regular criminal files and made available to any "authorized" agency which requests them.[11] Authorized agencies include not only state and local law enforcement agencies, but licensing bureaus, the Civil Service Commission and other government employers, private banks and other non-law-enforcement organizations. Thus, in spite of protective juvenile expungement and sealing laws, juvenile records are almost as widely disseminated as those of adults who have been arrested or convicted.

Incident: The Maryland Data System for the Handicapped[12]

In 1971, six Maryland state agencies--Education, Juvenile Services, Welfare, Retardation, Mental Health and Preventive Medicine--combined forces to contribute identified data on all handicapped children to a central computer file. Handicap was defined to include not only physical problems such as hearing and vision disorders, but "personality disorder," "major affective disorder," "sexual deviation," and "adjustment reaction." About 10% of the school age population was expected to be covered. One of the ways in which the data was to be collected was by distributing forms to public school teachers who would be asked to fill them in for each child in whom they observed one of the listed problems. The matter first came to the attention of civil liberties groups when several Prince Georges County teachers refused to fill in the form because they felt they were not qualified to make medical or psychiatric judgments.

The Data System for the Handicapped (DSH) was intended, state officials said, to collect data from the participating state agencies for research purposes only. One state official stated that it would help the state determine what resources needed to be allocated to special facilities for the education of handicapped children.

Originally, the ACLU of Maryland was a member of a Parent Interest Group Advisory Committee for the DSH system. However, it withdrew from that committee in 1974 because it concluded that the system as it was set up was not dealing adequately with the privacy and confidentiality problems involved. It charged that the system did not provide parental notification or review of the record created on a child; did not consider the right of minors to control these decisions themselves (rather than parents) where the minors are of sufficient age; did not assure periodic updating of records; did not secure parental consent to inter-agency exchange of records; and had not developed methods to compile the statistical data desired without placing names or other unique identifiers in the central file. Noting that it had received dozens of complaints from parents and professional groups about the system, and that "improper labelling" seemed to be an integral part of the operation, the ACLU called upon the state to halt operation of the DSH system until proper standards and procedures had been developed.

The state responded to the ACLU (and to the protests of several counties) by announcing that it was going to file records only by a code number, not by name; that data would not be furnished to outside agencies, and that consent and access was not relevant since only statistical uses were intended. They also promised to re-examine their labels, and to consider creating more precise categories. These were valuable changes, but the ACLU of Maryland still considers the DSH system to be insufficient in its safeguards.

Comment

The problems here are three that we have previously identified: (1) the concern over later inter-agency interchange; (2) the short-hand terms to facilitate computerization which may distort the meaning of the diagnosis; and (3) the collection of medical data by individuals who are not qualified to make medical judgments. There is, however, an accompanying societal problem to which we have already alluded at several places in the report, that computerization of identified medical records is declared necessary to provide a desirable benefit to the individuals about whom the information is being gathered--in this case, to provide resources for the education of handicapped children - but such a benefit is not forthcoming, at least not yet in Maryland.

Incident: The Maryland State Abortion Surveillance Unit [13]

In Maryland, the State Abortion Surveillance Unit, part of the state Center for Health Statistics, began in 1968 collecting data on women having abortions in the state, for "descriptive, planning, and evaluation purposes." 1968 was the year that Maryland law was liberalized to permit abortions for mental as well as physical health reasons, and the state decided that keeping statistical data on the number of abortions, the ages and demographic characteristics of the women, etc. was a major new concern for health analysts. This belief was strengthened when abortions in Maryland went up substantially, following the 1972 Supreme Court decision striking down restrictive state anti-abortion laws.

However, the activities of the Abortion Surveillance Unit drew heavy fire in 1974 from the National Organization of Women, the Children's Defense Fund, and the Maryland ACLU. Representatives from these groups noted that while the name is not included on the form issued by the Unit, it did require the patient's block number address and hospital case number (which was often the patient's social security number), and patients were not informed of or asked to agree to the sending of their data to the state Unit by doctors and health institutions. "These files are there so that at any time someone could make an administrative decision to share the information with another agency," said J.B. Dillingham, of the Children's Defense Fund. In addition, critics noted that many women felt quite uneasy about the idea that a state file kept a permanent record of their abortions. The form also included the notation whether the reason for the abortion was "elective, physical health, mental health, rape, congenital defect, or other," which was also considered an intrusive element about the patient to be kept in the state system.

Dr. Frances Warthen, director of Maryland's Center for Health Statistics, defended the program as one that was necessary because hospitals prior to the surveillance-report requirement often submitted "incomplete" yearly tabulations. She also explained that the block number and hospital case number were not entered into the computerized file; the block number was used only to place the case within a given census tract for statistical reporting, and the hospital number was obtained "should the facility need to be contacted for more information about a particular patient."

These explanations--especially the vagueness as to future uses of the hospital number--did not satisfy the critics. After consulting with them, Dr. Warthen agreed that the block address and patient identification number would be crossed off the form once the information was fed into the computer. In that way, she said, "there are no identifiers on any tape that also contains medical information." Protest over this activity still continues, however.

Incident: The New York City Fetal Death Registry

In New York City, a test case by a physician and his patient, supported by the New York Civil Liberties Union, led to a lower court ruling in 1972 striking down a city requirement that the name and address of the patient be provided to the city fetal death registry by the physician in all cases of medical abortions. The patient complained that furnishing her name and address invaded her privacy by intruding into one of the most intensely personal aspects of a woman's life; it also forced the physician to breach a confidential communication. The court observed that there was no statutory direction that the name and address be put into the registry, and no proof made out that the city needed this for statistical and public health purposes, yet the requirement had the effect of jeopardizing the state's liberalized abortion policies. The court held that compelling disclosure of name and address was "arbitrary and capricious," an "unlawful invasion" of the patient's right to privacy, and an improper interference with the "clearly cherished right of absolute confidentiality of a physician-patient relationship."[14]

In December of 1975, the New York Court of Appeals reversed that ruling in a 4-3 decision that upheld the city's power to require physicians to report the names and addresses of all women receiving abortions to the central fetal death registry.[15] The majority found proper and "laudable" the city's purposes to monitor procedures, facilitate follow-up of complications, track possible adverse effects of abortions, and offer family counseling. The fact that the U.S. Supreme Court had upheld the constitutional power of states to adopt regulations for abortions during the second trimester of pregnancy was considered support for the city's action. In the absence of any allegations that the information was being used improperly or being disseminated for other purposes, the majority said that there was no infringement on the right to abortion or of the patient's right to privacy.

The dissenters felt that "the right to privacy which the Supreme Court extended to a woman's decision to abort necessarily extends to and includes her right to guard her identity from a centralized abortion registry." They noted that all the purposes sought by the city could be accomplished by using either files in the hospitals or statistical reporting to the registry. The case is now being appealed to the U.S. Supreme Court.

Problem: Child Abuse Registries [16]

One area in which the central registry idea has taken hold with particular firmness in the past decade is child abuse. In 1966, only four states had central registers to which instances of child abuse were reported; by 1974, 30 states had passed laws requiring such registers (in varying forms) and many local governments had enacted them as well. The laws generally require doctors, hospitals, school officials, welfare officials, and other professional groups to report wounds and injuries sustained by children. Some of the registries allow any individual who wishes to volunteer a report of child abuse. During the past few years, while approving the general purpose of protecting abused children, civil liberties and other citizens groups have opposed drafts of such child abuse registery laws in some states when these lacked sufficient provision for due process hearings before adults were listed as child abusers; when the system could lead to "potential blackmail;" when case reports that might be based on shaky evidence would be available to various public officials such as the police, welfare administrators etc.; and when "a permanent computer file of an alleged child abuser could follow him around all the rest of his life." In several cases, protests by civil liberties groups resulted in the enlargement of safeguards in the enabling legislation, and were then enacted.

Problem: Drug Prescription Registries

During the early 1970's, many states enacted laws requiring dispensing physicians or pharmacists to send the state a form whenever they dispensed certain drugs having "high potential for abuse." The specified drugs included not only morphine and codeine but also ritalin, percodan, and hucodan; these drugs are widely used in treatment of obesity, high blood pressure, hyperkinetic children, epilepsy, migraine headaches, and other "regular" medical problems. The compulsory report includes the name and address of the patient.

New York enacted such a law in 1973, and set up a computerized "controlled drugs" registry in Albany maintained by the State Bureau of Controlled Substances, Licensing, and Evaluation. The registry's purpose, according to the State, was to identify persons who obtained multiple prescriptions or received more than a 30 day supply of these drugs. After 20 months of operation, the registry had about two million prescriptions recorded.

Several groups in New York--the Empire State Physicians Guild, the Legal Action Center, and the New York Civil Liberties Union--brought suit in federal court to have the registry law declared unconstitutional. A federal court of appeals held it unconstitutional in 1975 as an unjustified invasion of the privacy of the doctor-patient relationship.[17] At the court hearing, several patients testified that they stopped taking the designated medicines when they learned that they were being recorded in the state registry:

> "A cancer patient using percodan for pain stopped taking the drug when he learned of the registration. He tried other drugs which did not relieve his suffering, and now orders the drug through his union from sources outside the state."
>
> "Another patient said she had used a medication containing codeine for migraine headaches, but when she learned that her name would be reported to Albany and put on a computer, she stopped the medication."
>
> "A woman whose child suffered from hyperkinesia took the child off ritalin rather than have him 'branded for life' as a drug user."

The court said the issue was a "troublesome" one, since the state was trying to deal with the very real problems of drug abuse. However, the court noted that only one person going from doctor to doctor for prescriptions had been found in 20 months; to compile a data base of over 2 million personally identified prescriptions for such results, the court said, was "too high" a price "in dimunition of freedom."

"An individual's physical ills and disabilities, the medication he takes, the frequency of his medical consultation are among the most sensitive of personal and psychological sensibilities....One does not normally expect to have to reveal to a governmental source these facets of one's life. One is wont to feel that this is nobody's business but his doctor's and his pharmacist's."

To the state's argument that compiling a registry in Albany was no different from having the name and address on file with pharmacists the court replied:

"A name on a prescription in the files of one of the many thousands of pharmacists in the state is entirely different from one's name on a form in Albany which is transferred to computerized records and stored for instant retrieval."

A similar protest was mounted in Rhode Island in October of 1975, at a hearing held by the State Health Department to allow public comment on a proposal to set up a similar state registry of "high abuse potential" drugs.[18] The Rhode Island ACLU testified that this would create a derogatory data bank even though the individuals listed in it had all been prescribed legal drugs by licensed physicians. ACLU State Director Michael Dollinger said that he knew of no legal authority that would allow the state to "so invade the privacy of the doctor-patient relationship." He stressed that if the state wanted to detect over-prescribing or over-dispensing of drugs, and detecting theft or forgeries, this could be done by removing the patient's name and address from the reports, and monitoring patterns of doctor or pharmacist conduct. Even if the goal was to detect persons who go from doctor to doctor to get prescriptions, Dollinger pointed out that such persons could easily change their names each time, and thereby escape detection by the registry. As in the New York case, the Rhode Island ACLU presented testimony that some individuals had refused prescribed medication, against the advice of their physicians, because of fears of "being included in the state's data file of 'drug addicts'."

Problem: Narcotics Addict Registries[19]

Confidentiality of data in drug-abuse treatment programs has been a major area of controversy during the past few years, with automated files playing a growing role in the issue. Essentially, drug-abuse treatment centers represent a decision by their sponsors (and government funding sources) to follow a medical rather than criminal approach to addiction; preserving strict confidentiality for patient identity and case details is critical to the success of these ventures. This was recognized by the 1970 and 1972 federal laws on drug-abuse prevention and control. After providing federal funds for treatment, rehabilitation, and research programs, these laws afford protection for the identities and records of persons receiving treatment in federal-agency programs, or federally licensed ones, or drug research programs by state or private agencies, when these have been specifically designated by the Secretary of HEW or the Attorney General to be exempted from compulsion of participant identities in any federal, state, or local proceedings.

Most drug-abuse treatment centers are not so protected, however, and studies disclose constant pressures from police, licensing agencies, employers, and others to learn the identities of program participants.[20] Some of this pressure comes from requirements that physicians must report to the state the identity and status of every addicted person they are treating (1/3 of the states have such requirements). Many states also have narcotics-addict registries, based on reports of identified patients from physicians and treatment centers throughout the state. Some of these states, like New Jersey, have computerized their registers. Where federal or state agencies provide funding for treatment centers, they often insist on having identified patient reports sent to them for auditing and evaluation purposes, and these are frequently put into state central databanks. As a leading article on this issue by McNamara and Starr in the Columbia Law Review noted in 1973,[21]

> These centralized state and federal data banks of narcotics-treatment information are a great threat to confidentiality. Of the (172) treatment centers responding to our survey, problems in protecting client records were cited 50 per cent more frequently by centers located in states with centralized addiction registries than by those located in other states. The information sought from the centers included drug, criminal and medical history, social and demographic data, prior drug treatment information, and employment data.

The McNamara and Starr study noted that protecting the physical security of treatment center files was a problem for the managers; given available "sophisticated" procedures, the authors felt computerized records could be kept more securely than the usual manual records. But they also saw the compactness and ease of search of the file making computerized files particularly tempting to overzealous law enforcement agents and other intruders.

The study also noted that undercover police agents have been sent into some treatment centers posing as clients or applying for jobs, as a means of getting confidential information on participants. These situations suggest that protecting files, whether manual or computerized, would take special alertness to efforts at penetration from inside as well as outside.

Conflicts over the confidentiality of drug-abuse treatment records are still a major confidentiality issue today. In Cleveland, Ohio, the local ACLU in 1974 criticized operations of the county's central computerized registry for patients receiving methadone treatment. The registry's purpose was to prevent individuals from enrolling in more than one program. But the data collected (following federal regulations for methadone programs) included many sensitive items--age, sex, educational level, employment history, criminal history, past history of drug abuse of all types, and prior treatment for drug abuse. The Cleveland ACLU objected to what it felt were overbroad disclosure provisions for such data, and the conditioning of a government benefit on the individual's willingness to surrender his/her privacy. They also insisted that patients should have a right "to access and correct the file," which was not provided.

Similar protests, including lawsuits challenging such drug-abuse registries or funding-agency reporting duties, have arisen recently in San Francisco, Maryland, and New York, among others.[22] Two states in 1973--Massachusetts and Pennsylvania--refused to accept federal drug treatment funds as long as patient information required by a "Client Oriented Data Acquisition Process" (CODAP) had to be submitted to a computerized file maintained by the White House Special Action Office for Drug Abuse Prevention.[23]

The Massachusetts action is worth examining more closely. After the Governor informed the White House Office for Drug Abuse Programs that it would do without federal funds rather than submit patient identifying data, the federal officials exempted the state from that requirement. "If Massachusetts will take the responsibility for providing aggregate data," the director of the office said, "that will be all right with us." Massachusetts therefore kept personal identification data at individual drug treatment clinics or the state's Mental Health Department.

Massachusetts then found itself faced by another federal drug reporting demand. Project DAWN (Drug Abuse Warning Network), a project of the Drug Enforcement Administration of the U.S. Justice Department, calls on hospitals and crisis-centers to report drug overdose incidents. In 19[illegible] at the request of the White House Office on Drug Abuse, the DAWN project added to its reporting forms the following information: subject's birthdate, race, sex, the first two letters of the subject's mother's given name and her surname. Again, the Governor of Massachusetts refused to submit identifying data, saying that institutions in his state would not cooperate in the DAWN project if these were required. The Governor's spokesman called the identification requirements "a bad, ill-advised program."

Massachusett's protest led Senator Sam Ervin Jr. and the Senate Subcommittee on Constitutional Rights to call the federal drug program officials before it in 1973, raise the citizens rights issues, and call on the administration to reconsider. Senator Ervin reported to Congress that "once the agencies reconsidered, they decided that they could get along without the objectionable information after all. Their data-gathering continues, but a small blow has been struck for better, less obtrusive government."

Comment

Computerized central registries organized around a single theme--child abuse, abortion, drug abuse, etc.--present in another form all of the problems we have previously catalogued. This is because a central registry is by its nature a governmental catch-all. Some agencies with access to the registry--or ready to seek access--will see it as invaluable for research; others for providing rehabilitation and social services; others for eligibility decisions or to avoid duplication of benefits; and still others for law enforcement purposes. The registries, typically, are created because there is general agreement that society has a difficult problem that it must solve and that the first step toward a solution must be identification of those either suffering from, or participating in, the problem behavior. These generally accepted perceptions lead to the creation of a central registry, and since computerization facilitates collection of such data, the move to central registries has been heavily accelerated by computerization in the past few years.

Although there is often public agreement that a central registry is a good idea, there is less agreement as to which of the above-listed purposes it should serve, generally because social viewpoints differ as to the larger question of how the problem should be solved. As a result, such registries tend to collect all the data they can on a particular subject in order to serve each of the various government agencies, should the occasion arise.

The ill-defined goals tend to be reflected in ill-defined limits as to the identification of individuals, what data is to be collected, who contributes to the collection, and rules for dissemination. A distinctive feature of some registries is that unidentified persons may contribute unsubstantiated incidents of what they regard as questionable behavior. This is true of most child abuse registries and of some drug abuse registries.

Incident: The Texas Central Data Bank [24]

In 1974 Texas announced that it was establishing a computer file at the state level that would pull together and record all the state "client" services an individual is receiving. Each record would have name, Social Security number, race, and date of birth among its personal data, and then contain a summary of state services being provided--health, mental health, rehabilitation, blindness, alcoholism, probation, welfare, employment, college and university, retardation, youth services, and others. Governor Dolph Briscoe explained that the state services index was needed to eliminate duplicate applications, coordinate provision of services, and improve overall state planning and organization of social programs. The ACLU of Texas and other citizens groups criticized the program on the ground that existing federal and state laws or regulations expressly provide for the confidentiality of some of these services, and that opening the index to state officials--even just the listing that someone was receiving a "service"--could be highly intrusive. John Duncan, executive director of the Texas ACLU, warned that "the plan creates the potential that with the press of a button, a nosy dean can find out if a student has received psychiatric services from the Department of Mental Health, or a prying bureaucrat in the Employment Commission can find out if a person was a juvenile offender years ago."

The Texas ACLU also criticized the "consent" feature of the state plan. When state officials noted that a service-recipient's consent would be required before his/her name would be entered in the index, the ACLU replied that agreement would rarely be uncoerced under these circumstances. "What individual who has received services from a mental health clinic, been confined in Texas Youth Council facilities, been treated for alcoholism, or received food stamps would freely consent to having this information float from agency to agency via computer?" In early 1975, Texas abandoned this plan because of lack of funds.

Incident: Wisconsin Central Data Bank [25]

Similar multi-file databanks at the county and city level have also drawn fire on citizen rights grounds. In Wisconsin the state Departments of Health and Mental Hygiene proposed in 1974 that counties using state-services should place in one computer file information on each individual in the county using a state-financed service for mental health, alcoholism, drug abuse, or mental handicap. Instead of four separate record systems, as previously maintained by the county agencies involved in furnishing these services, there would be one set of forms for all the services--admissions, evaluations, scheduling, etc.,--and one information system for storing and using the data. Client numbering would be changed so that only one client number would be used regardless of the service provided. The client number and case data on clients would then be sent to the state's computerized file for program evaluation, auditing, etc.

When this proposal was presented in Milwaukee by the administrator of the County Unified Services Board, it drew strong opposition from mental health agencies, social services groups, and the Wisconsin ACLU. When the plan was first announced in May of 1974, the ACLU consulted with state and county officials and concluded that no overriding need for the data had been demonstrated that would justify the threats to privacy and confidentiality, and it called for a halt to implementation of the databank. The ACLU set out a list of safeguards that it felt should be provided before such a system should go forward:

1. The right to inspect any information about herself/himself in the record system.
2. The right to contest the accuracy of the information, to correct errors, and to have such corrections recorded in the file and reported to all those who have received the wrong data.
3. The right to place explanatory information in his/her file.
4. The right to know the administrative policies and procedures governing the maintenance and use of her/his file.
5. The right to know the remedies available to her/him when he/she wishes to challenge information. Individuals should learn this information from the agency at the earliest opportunity after the decision has been made that a file will be kept on the person's case.
6. The right to be heard in person on any substantial issue concerning the record and the right to a statement of reasons if a decision unfavorable on the claim of the individual is made.
7. The citizen must be notified upon each release of information to an outside agency or party and upon any inter-agency transfer of records.

In August of 1974, the administrator of Unified Services presented a revised proposal for a county index. A computer program would transform a client's name and birthdate into a number and would store records under that number, but would not have the name connected with the data. Each agency under contract to the Board would have a terminal in its offices so that it could put the client's name and birthdate in and get a number back for record purposes. Only the individual agency would know both the name and the number, and reports on clients sent to the state's computer system would be identified only by number. To catch duplications--perhaps the prime purpose of the unified data system--coordinators at the county computer operation would check when names were submitted for numbers to see whether other agencies had reported having that individual with them, and would check to see whether this represented "unnecessary duplication of services."

This revised system was still opposed by the groups that had criticized the earlier plan, including the Mental Health Planning Council, Alcoholics Anonymous, and the Wisconsin ACLU. The terminal feature, they said, would mean that employees and anyone else who could gain physical access to agency offices could play with the numbers-and-name system, and that there still had been no proof shown that a single numbering system on clients was necessary to plan services and avoid duplication.

Comment

The Central Databank concept translates into reality the previously expressed fears of critics about controlled dissemination of identified information from one government agency to another. The recounting of the events surrounding the creation of these two data banks, and the debate over the adequacy of notice, consent, challenge, and correction in such systems highlights the citizen rights problems these types of systems present. One point about such central data banks deserves special emphasis. It is a point that we have noted in passing when describing smaller computerized systems, but that has a special relevance for a large, complicated multi-level data bank. The process that takes place here is that first the databank is created; then protests arise from civil liberties groups and professional associations; then the government agency often tries to make some accommodation to the complaints, usually with limited success. The accommodation is bound to be of limited success because the reforms are tacked on as an afterthought, and are not really viewed by officials as an integral part of the system. Until and unless such citizen rights considerations are included in the earliest planning for data banks, seeking the widest acceptance from all segments of the community, recognition given later will be regarded by critics--rightly--as something grudgingly granted, and distrust will greet even well-meaning efforts by government officials--as an afterthought--to safeguard these systems properly.

In discussing the problems connected with various computerized systems, we have focused primarily on the lack of protections for confidentiality; less attention has been given to the questions of an individual's right of access. In only half a dozen of the episodes recounted here was the question of access raised at all by concerned groups; in only two of them was it given equal weight or more weight than protests about confidentiality. This conforms to the patterns already established with manual health records, where fewer protests have traditionally been made over lack of access than over breaches of confidentiality. However, in the past few years, there has been a growing consciousness that individuals do have a right of notice and access when records are collected and used to make governmental or consumer judgments about them.

But in the cases of computerized health records we have been discussing, most of the individuals whose records are included are probably not aware of their existence. A right of access--even if it were to be established--would be meaningless unless accompanied by the right of notice, and this raises several troublesome questions:

1. Most individuals receiving care in hospitals and clinics know that summary information about them--length of stay, diagnosis, identifying material, etc.--is being recorded about them by primary care providers. But patients usually have no idea it is being computerized and sent outside the facility for various "special uses." Several of our episodes, such as the fetal register and the abortion register fall into this category.

2. Most individuals seeing private physicians know that detailed sensitive information confided to their doctors may be recorded by them. But they have no idea that some of this sensitive information is also being computerized and forwarded to state health agencies. The New York State Department of Hygiene and Missouri data reports fall into this category.

3. There are situations in which individuals have no idea that information or judgments (whether medical or pseudo-medical) is being recorded about them at all, and no idea, therefore, that such judgments are being centrally computerized. The Maryland DSH system and those child abuse registries without notice provisions are examples of this.

4. There are individuals who have an affirmative reason to believe that information about them is not being recorded and transmitted elsewhere, as is the case with juvenile offenders who fall under the protection of the Youthful Offender Act and its state counterparts, but such persons are mistaken in their belief.

For a concept of adequate notice to be effective, it would not only have to inform the individual that personal information was being forwarded to a named centralized data system, but would also have to indicate what other agencies have access to it, so that the individual might know where his/her records are which might require correction or updating.

We noted, when discussing manual records, that the greater the dissemination of medical records into areas where they played an evaluative role--in employment, licensing, law enforcement etc.--the more important was the question of access, with the opportunity to correct errors. Centralized computerization heightens this importance in direct proportion to its greater capacity to disseminate personal information to a broad variety of agencies and institutions which make such evaluative decisions.

Two special problems of computerization that do not fit into the categories already outlined deserve mention here:

Incident: The California and Michigan Beneficiary Explanation Programs[26]

Improper or fraudulent claims by doctors have been a concern of the federal Medicare and Medicaid programs since their inception, as well as of state supplementary payment programs such as California's MediCal. To improve the efficiency and monitoring of claims processing, the Federal government pays any state that installs an approved computerized claims processing and information system 90% of the cost of installing the system and 75% of its operating costs. One of the conditions the state must meet is a "beneficiary explanation program" in which a notice is sent to the home of recipients listing the medical service reported to have been performed and requesting recipients to notify the state if any of these services were not, in fact, delivered.

The beneficiary explanation program has been used extensively by states such as Michigan and California as part of their computerized claims processing systems. In a four month period in Michigan, for example, the state sent beneficiaries 1.7 million such forms.

In 1974, two 15 year old girls had medical abortions paid for by MediCal. Joined by several organizations, the two girls sued in federal district court to enjoin California from mailing notices to their homes. They charged that the notices for all MediCal recipients in a given household were sent in a single envelope, and that the abortion information would thus be available to their parents, even though California law protects the right of minors to abortion (and other medical treatment without parental notice or consent. The lawsuit, filed as a class action, it contends that the beneficiary notification program would "discourage poor women from obtaining necessary medical services such as venereal disease treatment, contraceptives, pregnancy or abortion services, drug and alcoholic treatment, or psychiatric counseling."

The lawsuit also charges that the results that had been achieved thus far under the recipient notification program did not justify its invasive aspects. Out of the 1.7 million notices sent out in Michigan, only 2,100 produced communications from recipients raising questions about the services listed for them. Paul Allen, director of the Medicaid administration for Michigan declared that the program has not "proved cost effective."

Comment

This seems to be a minor organizational problem, requiring more sensitive procedures (such as using first-class mail for the notices) and more sensible methods (such as using random sampling in selecting records rather than wholesale mailings). It is noteworthy because it is yet another instance of how consciousness of citizen rights issues in the planning stages could have avoided controversy.

Incident: The Maryland Drug Abuse Administration [27]

In March of 1974, the Baltimore press reported that several employees of the Maryland (State) Drug Abuse Administration(DAA) had been arrested by city and state police and charged with drug violations involving use of narcotics "at or near the drug abuse headquarters." The news stories disclosed that an informant had notified the director of the DAA several months previously that some employees of the agency had been using narcotics at "a party." The Director, I. Robert Evans, consulted with Dr. Neil Solomon, head of the State Health Department, who informed Governor Mandel of the situation. The decision was made to send an undercover state police agent into the Drug Abuse agency, posing as an employee working in the planning section. He worked there for approximately six weeks, and information he developed led to the arrests.

These disclosures led to a series of meetings in March and April by representatives from local and statewide drug and alcohol treatment programs, medical groups, hospitals, and the Maryland ACLU, based on threats to the confidentiality of client information posed by such undercover activity. A Maryland Committee on Client Confidentiality was formed, and a statement issued that called on the Governor to see that no undercover agents would thereafter "be introduced into any phase of the Maryland drug treatment and rehabilitation system." The Statement explained that these organizations "do not condone nor do they wish to defend the alleged illegal use of drugs by the individuals arrested." However, placement of a police undercover agent in the state drug abuse treatment agency disrupts the "trusting relationships" between client and counselor, and among agencies; jeopardized the security of the drug-abuse registry and other confidential records kept at DAA; and "demonstrated judgment incompatible with continued trust of the Drug Abuse Administration by local programs."

In meetings with the concerned groups, DAA Director Evans stated that using an undercover police agent was "the best investigative method" possible and "the only way to root it out." He said that the agent had been given "specific instructions" not to have anything to do with client records and other confidential data. In fact, he added, the staff members arrested, because of their drug use, were unreliable persons to continue to have access to the confidential information.

These explanations were not considered adequate by the protesting groups and the controversy deepened. Dr. William C. Ebeling, head of the state university medical faculty and its medical society, sent Governor Mandel a communication charging that employees of DAA had made certain records from the confidential Narcotic Addict Registry available to the agent. (The registry lists all persons being treated in 60 centers throughout the State.) Dr. Ebeling's complaint, plus those of 13 private drug treatment programs, led the state health department to order an investigation of the incident in early April.

As a result of the investigation, authority over record-keeping by DAA was shifted from the agency's director to its medical director, Dr. Samuel L. Fox. Dr. Fox announced in August of 1974 that he was destroying all records accumulated by DAA over the past five years that identified drug users by name, leaving the originals of those records only in the local programs. He also modified proposed DAA regulations which would have required names to be sent to the state and set up a coding system instead. The Maryland Association of Mental Health and other groups hailed the new policy, and John Roemer, director of the state ACLU, praised the decision as "a large step forward in protecting both privacy and rehabilitation."

However, the question of whether police would be used in the future as undercover agents in drug programs and other sensitive social-rehabilitation programs was not addressed by the Governor, or any state health officials. John Roemer noted that the 1974 incident ought to be a warning that no state registry or record-system could be considered secure and its data confidential if the "needs of law enforcement" prompted its keepers to allow such undercover penetration by the police. "There is no guarantee that such an agent would not look at the records if that would help in the investigation, and it would be almost beyond human nature for such an agent to resist a peek at the files for a wide range of police investigation."

Comment

We have tried to avoid as far as possible the "what if?" approach to computerization, and to confine our analysis to factual episodes. However, the placement of an undercover agent in the proximity of supposedly confidential files speaks to all the fears generated by the Nixon-White House plumbers, the burglary of Dr. Fielding's office, and the complex of issues raised by Watergate. It cannot help but evoke the question: What if the need were compelling enough--say a threat to the President's life, or the danger of a mass terrorist bombing? Would any system, even one like MSIS, protected by special statute, be secure against encroachment by law enforcement officers? And if such "appealing" situations were held to justify law enforcement access, then who among state or federal health officials would have the power--and the incentives and guts-- to inquire into the declaration of such "special needs" by law enforcement officials?

The answer to this and other "what-if" questions lies in the adoption of specific protective statutes, and of special review bodies to pass on requests for exemptions or exceptions. But it also requires a deepening of societal attitudes, through court decisions, greater public familiarity with the dangers as well as the benefits of computerization, and greater sensitizing of public officials directing government health and social services. The ways of fostering such attitudes will be discussed in the concluding section of this report.

Incident: The Medical Information Bureau [28]

So far, we have confined our reports to incidents of government computerization, which is where most public attention has been focused. But the problems of computerization are raised as well by some private organizations. As an example, we will return to the Medical Information Bureau, whose operations have been described earlier in Part I.

The MIB system was a manual, card-index operation for the first sixty-odd years of its existence; in the late 60's it was processing 10-15 million information requests annually from its 700 member life insurance firms. In 1970, MIB automated its files. It presently uses a service bureau in Boston to store data on some 11 million persons who have previously applied for life insurance, and to handle requests for reports.

There was no change, as a result of automation, in the kind or extensiveness of the data that MIB collected, stored, and distributed to its member companies. But the fact that MIB was not known to the public, and especially to individuals who might be denied life insurance or rated more highly by a life insurance company because of information supplied by MIB, prompted widespread criticism in the late 1960's and early 1970's from consumer advocates, civil liberties groups, and Congressional spokespersons. The fundamental criticisms were over the kind of "social data" that MIB had been collecting and disseminating (sexual behavior, finances, life style, mental "impairments," etc.); the lack of any provision for a person to inspect, challenge, and correct the information in his/her record; and the capacity of member life insurance firms who also write accident, health and auto policies to obtain use of MIB data for those purposes even though MIB rules said they should not do this. The fact that the Fair Credit Reporting Act of 1970 contained an exemption for medical data meant that MIB was not covered by the notification and access protections of that law, and this generated extensive criticism in hearings before Senator Hart in 1972 and Senator Proximire in 1973, and in both the medical and general press.

MIB reacted both slowly and defensively to these complaints. In November, 1974, it did stop collecting information about "sexual deviation" and "social maladjustment". In an interview in the Baltimore _Sun_ on July 13, 1975, Joseph C. Wilberding, MIB Executive Director, stated that the Bureau had voluntarily eliminated these categories from its "impairment" category. Instead, it substituted two new categories that would alert an inquiring company of the "existence" of such information. "All that is reported now," Mr. Wilberding explained, "is that company X thinks they got significant information from an unidentified investigative report. They are not reporting information, but they are reporting the possible existence of information that must be further checked out." This left many critics unimpressed.

In August, 1974 MIB announced that insurance applicants would henceforth be told in writing by MIB member firms that health data they supplied would be submitted to MIB for storage in its computer system and might later be shared with life insurance firms using the system.*

---

* Footnote on top of next page

MIB also provided that an applicant for insurance who wished to review his/her file might do so by asking that the information be forwarded to the insurance company to which the application had been made. That company would then make it available to the attending physician, who could review it with the applicant. Correction of any erroneous data would be made in general conformity to the procedures of the Fair Credit Reporting Act.

These procedures were still met by criticism. It was argued that the notice ought to be printed on the insurance application itself, and that access should be available to the individual directly, not filtered through the insurance company and through the "attending physician."

In 1975, MIB further broadened its access policies. Now, individuals could ask to see their MIB record directly, and could do so upon providing identifying data, and supplying a detailed history of previous insurance applications. Any"non-medical information"in the file would be released directly to the individual, by reversed-charge telephone call or personal appointment. Medical information would be disclosed only to the individual's personal physician. To obtain the medical information, a release had to be signed freeing MIB or its member companies from any liabilities or damages in connection with the information. This release applied to medical information released to the individual, and was based on the fact that MIB had no obligation under the Fair Credit Reporting Act to disclose its record to the individual.

To the criticism that medical records may be disseminated to unauthorized individuals or misused, MIB points to its rules that prohibit the transmission of medical information to life insurance companies unless accompanied by a signed authorization, and which prohibit life insurance companies from rejecting an applicant solely on the basis of a negative MIB report. In the interview cited above, however, Mr. Wilberding conceded that the Bureau has only two employees to review the 19 million requests for MIB reports each year, and that in a period of more than two years it was able to review the general procedures for compliance of less than 30% of

---

* An example of this new procedure is the notice used by Union Fidelity Life Insurance Company:

> IMPORTANT NOTICE
>
> Information regarding your insurability will be treated as confidential. Union Fidelity Life Insurance Company may, however, briefly report to the Medical Information Bureau on information received with your application. The Bureau*, on request from a member company to whom you may apply for insurance, or from whom you may claim benefits, will supply such information to the company. If you ask,the Bureau will arrange to disclose the information in your file (medical information will be disclosed only to your attending physician), and you may seek to correct any inaccuracy in accordance with the Fair Credit Reporting Act procedures.
>
> Union Fidelity Life Insurance Company may also release information in its file to other life insurance companies to whom you may apply for life or health insurance or to whom you submit a claim for benefits. Union Fidelity Life Insurance Company will not, however, reveal to another company, or to the Bureau, the action taken on the basis of your current request for insurance.
>
> *A non-profit membership organization of life insurance companies which operates an information exchange for its members. P.O.Box 105, Essex Station, Boston, Mass. 02112, telephone 617-426-3660.

its 716 member companies.

Comment

MIB first attracted attention in the mid-1960's, when legislative committees and writers on privacy began to publicize the presence of this central registry of medical and non-medical information for life insurance companies. Yet it was not until 1974 that MIB modified its use of "non-medical" data, and not until 1974 that it adopted policies for notice and access that meet what almost all observers would regard as fair procedures to protect the interests of life insurance applicants. That MIB is now taking some corrective steps is praiseworthy; but that it took agitation by critics for almost a decade to produce organizational responsibility does not speak well for MIB, for the life insurance industry, for the public officials in the state legislatures where MIB is chartered (Connecticut) or has its files (Massachusetts), or for Congress, which ought to have written careful provisions to protect consumer rights affected by the MIB data bank when it enacted the Fair Credit Reporting Act in 1970.

Incident: The Georgia "Free Consent" Experiment[29]

When government agencies computerize health and welfare client records, and when professional groups or civil liberties organizations raise questions about the confidentiality or security of the client data that will be stored, two typical responses are made by the systems managers: (1) only authorized personnel and legitimate users will have access to the data, and (2) the clients themselves are not worried about violations of the privacy of their records; this is mainly a case of overblown fears by self-appointed defenders. When it is pointed out that clients asked to give their consent to have health and welfare data sent to state computer systems do not really have a free choice--since they might jeopardize their benefits if they refused consent--the answer is that no one really objects.

An important experiment testing this assumption was performed at a Community Mental Health Center in Georgia during 1974-75. Before July of 1974, reports of services rendered by the community centers were sent to the State Division of Mental Health identified only by case numbers. For that reason, no need was felt to inform clients that information on them was being sent from the local center to "the state computers."

On July 1, 1974, Georgia directed mental health clinics and centers to send in for each new client his/her name, Social Security number, primary disability, previous mental health services, diagnosis, and other personal background data. Dr. Catherine E. Rosen, director of research and evaluation at the Northeast Georgia Community Mental Health Center (in Athens, Georgia) saw this as an opportunity to test how clients really felt about releasing their personal data. She designed an experiment that would see what clients would do if they felt they had a real choice in this matter.

The center's lawyer prepared a Medical Release Authorization Form that read as follows:

> "The undersigned patient hereby authorizes the Northeast Georgia Community Mental Health Center to furnish the Division of Mental Health of the Georgia Department of Human Resources a record or records including the following information: patient's name, social security number, and nature of patient's primary disability. Nothing herein shall authorize the Northeast Georgia Community Mental Health Center or the Georgia Department of Human Resources to release said records to the general public, as is prohibited by Section 40-2703, Code of Georgia."

During Phase I of the experiment, from July of 1974 to March of 1975, each of the 962 clients in the Center's four clinics were presented with the form and signed it. (Illiterate clients had it read to them, and clients too distraught to deal with the form on intake had it presented later). Compliance was 100%. No one declined to sign.

During Phase II, from March to September of 1975, the Medical Release Authorization Form was still given to clients to read. But then different additional procedures were employed. In two clinics, a "no option" statement was read aloud to the client. This said:

"The State wants to keep a record of name, social security number, and the type of problem of every person who comes for mental health services. The reason why the state wants this information is so that it can keep track of mental health services and clients throughout the state. If you sign this paper it means you give us permission to send in your name, social security number, and diagnosis into the state offices in the capitol, where it will be placed in the Mental Health computer file."

In the Center's other two clinics, this statement was also read but it was followed by an additional statement suggesting that the client has a genuine option. This stated:

"If you do not sign this paper, this identifying information will not be sent into the state offices in the capitol and will be kept only locally. In other words, if you don't sign you will get the same services from us as if you did sign."

In all the clinics, a pen was placed on the table after the reading of the statement so that the client could make his/her decision.

In the two clinics where 109 clients heard only the "no option" statement, compliance was 100%; everyone signed. But in one of the two clinics where both statements were read, compliance among 259 clients dropped to 41%. In the other, compliance among 104 clients dipped to 20%.* Analysis of the non-compliers showed them to be more often females and better educated, but there were not significant differences in other variables, such as age, race, income, apparent nervousness, severity of problem, etc.

---

*In the clinic scoring 41% compliance, a clerk presented the option: the clinic having 20% compliance had the clinician present it. Dr. Rosen believes that the willingness to withhold consent rose when the person who would provide the client with the mental health service he/she wanted said that there would be no lessening of service.

The spontaneous remarks made by clients when presented with the "option" statement left no doubt what was in their minds in refusing to sign. Concern was expressed about the effect of forwarding the information on the clients' current or future employment, possible loss of custody of their children, and fears about the information being used against them later for some government purpose.

Comment

Dr. Rosen's study provides striking proof of what civil libertarians have been asserting for years--that the millions of persons who are clients of government health services do care about the circulation of their personal data, and that their consent would not be freely obtained for many inadequately protected government data systems if clients really had adequate notice of what was to be done and felt they had a real choice of whether to consent or not. After Dr. Rosen's study, it ought to be suggested to every proponent of a sensitive data system, especially the computerized ones, that they administer the type of "real option" statement that Dr. Rosen used to a sample of those persons whose records would go into the system. Only when a substantial majority gave such consent should the proponents be allowed to assert that "people don't object to having their data in our fine system."

OVERALL CONCLUSIONS ABOUT "COMPUTER IMPACT"

All the incidents we have presented in this chapter arose from Zone 2 or Zone 3 activities--uses of computerized medical records or health data for utilization reviews or to make evaluative "non-medical" judgments about individuals. But the sources of the data in many such cases were computer files maintained by primary care providers in Zone 1, and thus collection and storage there has to be viewed in light of the demands for production of identified data being made by the Zone 2 and 3 activities.

Our analysis of these incidents suggests some almost painfully simple conclusions. Most computerized health data systems are being created or expanded without sufficient consultation in advance with groups representing citizens rights and doctor-patient interests, and without some kind of proceeding open to the general public. Most data systems lack sufficiently developed analyses of how much and what kind of identified personal data they really need to perform their function. Even when properly defined, most data systems fail to adopt sufficiently precise standards of confidentiality, controlling uses within the organization and releases of identified data to third parties. When it comes to rules for permitting patient access to their own records, very few computerized organizations have adopted procedures responsive to those patients who ask for and insist upon access.

Noting these general defects is not to say that there are no real problems of conflicting values or hard choices of social priority involved. Indeed there are, and that is what we will take up in our final chapter. But we approach this task of discussing alternative policies and making recommendations with the judgment that both citizen rights and effective use of computer resources require that we move away from ambiguous and ill-defined systems that leave people uncertain and fearful about their capacity to control the circulation of their medical and health data.

FOOTNOTES

1. Our sources for this account include: Letter from Eastern Missouri Task Force for Health Data Security to Dr. Herbert R. Domke, Director, State Division of Health, May 24, 1971; Vanessa Bush, "New Data Battle: States Need To Know vs. Patients' Privacy," Modern Health Care, May 1975, pp.60-61; Letter to Project from Mrs. Barbara Puder, R.R.A., October 28, 1974; "State Curb on Use of State Computer File," St. Louis Post Dispatch, September 24, 1974; Briefing Summary on the Missouri Discharge Survey Project, July 11, 1974; St. Louis County Medical Society Bulletin, June 14, 1974.
2. Detroit News, September 14, 1972 and April 15, 1973; Civil Liberties Newsletter, ACLU of Michigan, Fall, 1973, p.3.
3. Letter to Project from Lauren Selden, Executive Director, American Civil Liberties Union of Washington, October 3, 1972, with press releases and draft complaint enclosed.
4. Complaint, Volkman v. Miller, Supreme Court of the State of New York, filed January 23, 1973; note on the case being dismissed, Mental Health Reporter, June 1975.
5. Alan Taylor, "Precautions a Necessity for Dynamite- Like Data Banks," Computerworld, January 26, 1976.
6. Record on Appeal, Belmont v. California State Personnel Board, ACLU of Northern California, 1973.
7. Belmont v. Board, Opinion of the Court of Appeal of the State of California, First Appellate District, Division One, January 3, 1974.
8. "Welfare Caseworkers Protest Data Demand," Computerworld, January 12, 1976; Telephone interview with Lauren Selden, Executive Director, ACLU of Washington, January 21, 1976.
9. "Juvenile Offender Records: Open Secret," The Privacy Report, No.12, July 1974.
10. This discussion of Juvenile Records is summerized from The Myth of the Hyperactive Child by Peter Schrag & Diane Divoky, New York, Pantheon Books, 1975, Chapter 6.
11. Deposition of FBI Agent Beverly Ponder, in Menard v. Mitchell, 328 F. Supp. 718 (1971).
12. Sources include: "Handicapping the Handicapped," Bulletin of the Maryland ACLU, Vol. IV, No.III, June 1973; Letter by ACLU of Maryland to heads of six state agencies, May 14, 1973; "ACLU To Withdraw From Advisory Committee of the Data System for the Handicapped," News Release, March 25, 1974; "ACLU, Parents Ask Restructuring of Data System for Handicapped," Computerworld, June 19, 1974.
13. "Maryland Data-Collecting Agency Criticized," Washington Post, September 16, 1974; Letter, John Roemer, III, Executive Director, ACLU of Maryland to Dr. Jane Wharthen, March 26, 1974; Dr. Wharthen to Mr. Roemer, April 4, 1974.
14. Matter of Schulman, reported in New York Law Journal, August 2, 1972.
15. In re Schulman et al v. New York City Health and Hospital Corp., N.Y. Court of Appeals, December 4, 1975; The Privacy Report, Vol. III, No.6, January 1976, pp. 8-9.
16. Alan Sussman, "Reporting Child Abuse: A Review of the Literature," 8 Family Law Quarterly, December 1974; Rowine Hayes Brown, "Controlling Child Abuse Reporting Laws," Case and Comment, January-February, 1975, pp. 10-16; Alan Sussman, "Guidelines for Legislation; Child Abuse and Neglect Reporting," Juvenile Justice Standards Project, Institute of Judicial Administration, Inc., American Bar Association, September 1974, Final Draft, January 3, 1975; "Child Abuse Register Vetoed," Computerworld, June 7, 1972; " A Bill to Curb Child Abuse Stirs Debate," New York Daily News, April 26, 1973; New York Times, April 27, 1973.
17. "Court Voids a Drug Log on Patients," New York Times, August 15, 1975; Roe v. Ingraham, 357 F. Supp. 1217 (1973), 480 F. 2d 102 (1973), U.S. District Court for So. District, August 13, 1975; "Prescription Dossiers Proscribed," N.Y. Civil Liberties, November-December 1975.

18. *Rhode Island ACLU Newsletter*, October 1975; Memo from Michael B. Dollinger, December 25, 1975.

19. Robert M. McNamara, Jr. and Joyce R. Starr, "Confidentiality of Narcotic Addict Treatment Records: A Legal and Statistical Analysis," 73 *Columbia Law Review* 1579 (1973).

20. *Ibid*.

21. *Ibid*.

22. Items in Project files. The Cleveland episode came from a letter and enclosures from Gordon J. Beggs, Executive Director, ACLU of Greater Cleveland, August 6, 1974. On San Francisco see *Curry v. Brian*, Complaint 689-724, filed in Superior Court of California for the City and County of San Francisco, and Harriet Katz Berman, "Addicts' Rights," *Civil Liberties*, No.304, September 1974. For Maryland, see Statement of ACLU at a hearing on "Guidelines Governing Residential Drug-Free Treatment and Rehabilitation Programs," Maryland State Drug Abuse Administration, January 25, 1974.

23. *Computerworld*, August 15, 1973, August 29, 1973, September 19, 1973; Thomas Land, "An Addict's Right to Privacy," *Data Systems*, June 1974, pp. 28-29; "Report on Privacy Case Study Published," *Congressional Record*, November 25,1974, Statement of Mr. Ervin.

24. *The Privacy Report*, Vol. II, No.1, August 1974; "Texas Group Opposes Interagency Data Banks," *Computerworld*, October 23, 1974.

25. Memo from William A. Lynch, Executive Director, Wisconsin Civil Liberties Union to William F. O'Donnell, Unified Services Board of Milwaukee County, on "Centralized State Data System for Unified Services Clients," July 3, 1974; "Agencies Reject Computer System," Milwaukee *Journal*, August 9, 1974.

26. "Rights Suit Seeks To Bar Data Plan," New York *Times*, December 1, 1974.

27. Baltimore *Sun*, March 12, 13 and 14, 1974; "Report on Meetings in Howard County with L. Robert Evans," March 20, 1974; "Report on Meetings Regarding Arrests at the D.A.A.," March 25, 1974; Statement of the Maryland Committee on Client Confidentiality," April 3, 1974; Baltimore *Sun*, April 4, 1974; August 22, 1974; Telephone interview with John Roemer, III, Executive Director, ACLU of Maryland, August 1975.

28. Benjamin Lipson, "Confidentiality in Life Insurance Underwriting," Paper prepared for Conference on Confidentiality of Health Records, Key Biscayne, Florida, November 1974; Richard D. Lyons, "Insurance Data Called Faulty," New York *Times*, October 4, 1973, p.22; "Small Step Forward," *Computerworld*, September 4, 1974, p. 8, "Insurance Data Bank Attacked as Abuse of Confidentiality" *Hospital Practice*, August 1972, p. 47; *Commercial Health and Accident Insurance Industry, Hearings Before the Subcommittee on Antitrust and Monopoly of the Committee on the Judiciary, United States Senate, Ninety-Second Congress, Second Session, Part I Pursuant to S. Res. 256, Section 4*, Washington D.C., U.S. Government Printing Office, 1973; "Medical Records: They May Be Bad For You," New York *Times*, October 7, 1973; "MIB: It Has 12 Million Americans at Its Fingertips," *Prism*, June 1974, p.29; "Doctor, Patient, and the Insurance Company: Abuses of Medical Privacy," *The Privacy Report*, Vol. II, No. 3, January 1975, page 2; "'The Medical C.I.A.'," *The Privacy Report*, April 1974,p.5; Nancy French, "MIB Medical Data Bank Institutes Notification, Inspection Rights," *Computerworld*, August 28, 1974, p. 1, Paul S. Entmacher, "Computerized Insurance Records," *Hastings Center Report*, November 1973, p. 8; E. Drake Lundell Jr., "Medical File Data Bank Investigated," *Computerworld*, June 7, 1972, p. 1; Leonard Sloane, "Personal Finance: Health Data Units," New York *Times*, January 13, 1975, p. 45; "Data Taps Threaten Patient-MD Bond," *Medical World News*, June 1, 1973.

29. Catherine Elkin Rosen, "Why Clients Relinquish Their Rights To Privacy Under Sign-Away Releases," draft of report sent to Alan Westin, December 31, 1975.

CHAPTER 12. COMPARISONS WITH OTHER DEMOCRATIC NATIONS

Before considering policy alternatives, it is helpful to compare American developments with regard to medical automation and citizen rights with trends in other democratic nations. While we did not study the situation in other countries with the intensity that we did for the United States, we did develop a combination of published sources, personal interviews, correspondence with government health agencies and medical societies, and visits to selected countries on which to base some useful comparative observations.

Health care patterns reflect national cultures. Among advanced industrial nations with parliamentary institutions, this leads to diversity, for example, in how much of the gross national product is put into health care, how the health delivery system is organized and financed, the scope of services made available to the citizenry if there is a national health insurance plan, the roles played by central and local government, the type of administration over public and private health institutions, and the degree of regionalization that is used for health services. There are also important differences in law and administrative tradition among democratic nations that will affect automation in health care, as with the presence in countries such as Sweden and Israel of a national citizen number that facilitates record linkage along regional or national lines.

Along with such national differences, there are also many common elements in the health systems of industrialized democracies. The percentage of gross national product spent on health care has been rising steadily in these nations during the past decade, along with public expectations that providing access to health care is a public responsibility. A concentration on preventive medicine, outpatient care, and regional coordination has also been common to many national scenes. More generally, the concepts of medicine, the organization of practice into specialties, and techniques of medical procedure are widely followed in Western societies, while the status and attitudes of medical professionals as an occupational group and the organization of hospitals and clinics as institutions also exhibit many similar characteristics.

The tradition of medical confidentiality--the doctor-patient bond--is a common Hippocratic heritage expressed in the ethical codes and legal systems of each Western nation. In addition, all the democracies have had concerned public debates during the past decade over the impact of advanced technology on privacy and citizen rights, so that a general sensitivity to this issue has become part of the political culture in each of these nations.[1]

Dissemination of computer technology has also been a multi-national force. The major computer manufacturers and developers of software systems operate throughout the industrial nations, spreading machines, systems concepts, and tales of successes and failures as part of their marketing endeavors. In addition, international conferences of health professionals and medical automation specialists exchange techniques and experiences with each successive generation of computer systems.

As we examined computer development abroad, we found the same pattern of leading-edge systems, mainstream users, and low-level users as in the United States. Both from our observations and the commentaries of technical and medical experts, it was clear that no country as yet has a single computerized data system integrated throughout its national health care programs. Most leading-edge applications are within single hospitals, or in local (regional) health-service delivery areas, or in their regional or national health-payment plans. Even these applications are usually described by their developers as still "experimental;" none have yet filtered down to common practice in the clinics, hospitals, health plans, or government health services of any country.

Leading-edge applications in most European nations do begin with a greater role for national or regional government than is true in the U.S., either through a socialized medical system or a national health plan. This puts most other democratic governments in a more direct role vis-a-vis the funding and evaluation of computer applications in health care. In addition, government agencies are often the direct managers of regional health data systems that maintain a record about the health of each resident in a city, county, or similar unit. Here the availability of official citizen identification numbers has played a major role.

Within hospitals, either as single institutions or as cooperating members of a consortium sharing a common computer system, the pattern of applications being pursued in Europe parallels closely what we have described in American hospitals. A few hospitals are pursuing unified hospital information systems, and report themselves in much the same modularly-developing situations as Kaiser-Permanente, Massachusetts General, or the Texas Institute for Research and Rehabilitation. Other leading hospitals are pursuing discreet applications, such as automated multiphasic health testing, problem-oriented patient records, cardiac display, nursing station systems, and the like.[2] The great majority of computers in health care in all these nations is still devoted to accounting systems and administrative reporting.

With this brief overview we will turn to a discussion of how medical automation and citizen rights activities are developing in six democratic nations: Britain, Canada, West Germany, Australia, France, and Sweden.

Great Britain

The National Health Service (NHS) provides universal, comprehensive medical care for all residents of Great Britain. The patient's point of entry into the system is the family physician, a general practitioner whose government remuneration combines a basic practice allowance, fees for specific items such as maternity service, and capitation fees. Approximately 98 percent of the population is registered with a National Health Service doctor.[3] A few private health insurance programs have been retained and are generally used to obtain the services of consultants or benefits such as a private bed in a public hospital.[4]

The 1972 NHS expenditure (£2,832) represented 5.06 percent of Britain's GNP.[5] Over 85 percent is financed through general taxation. A little less than ten percent of the balance comes from workers' and employers' National Insurance contributions, with the remaining amount coming from services requiring cost-sharing, such as dental treatment and charges for private beds in public hospitals.[6]

The Department of Health and Social Security is responsible for the administration of NHS, which was extensively reorganized in 1974. Currently the basic unit is the District. It supplies 250,000 persons with community health services, supported by the specialist services of a district general hospital. The Area Health Authority is the primary level of statutory authority with planning and operational responsibilities. Fifteen Regional Health Authorities, under national policy guidance, allocate resources to the Area Authorities.[7]

NHS physicians may practice alone or in a group, and over half the family doctors are members of partnerships.[8] In 1972 there were 54,500 physicians in Great Britain, a ratio of one per 1,000 population.[9] About half the general practitioners see private (non-NHS) patients, but only five percent have more than 100 such patients.[10] The number of hospital beds in 1971 was 508,000, a ratio of 9.4 beds per 1,000 population.[11] During the 1962-1971 period, in-patient cases increased by 19.7 percent, but the average time spent in hospitals by in-patients fell from 33.46 days to 23.87, a 29 percent reduction.[12] New out-patients rose by 9.1 percent. The proportion of private beds in hospitals is one percent, and the number of private patients treated is usually just under two percent.[13]

Enthusiastic predictions in the middle 1960's about the extent to which computers could be utilized within the British health care system have been tempered with time and the complexities of experience. While the British remain active in their search for computer applications, the Department of Health and Social Security has recently instituted an evaluation program for potential applications based on a three-step process of experiment, development, and implementation.[14] Though this cautious approach has become the norm, most observers note that the place of the computer in the delivery of health care is secure. As one expert recently stated, "In contrast with the situation a decade ago, when a computer might be considered an optional extra within the Health Service, computers today play a vital role in many Health Service activities and their future potential appears virtually limitless."[15]

There are three principal types of medical computing activities in Great Britain: (1) large batch processing installations concerned with routine finance and national information systems; (2) small installations usually dedicated to single applications and associated directly with medical science, pathology, radiotherapy, etc.; and (3) hospital-based information systems that would be considered "leading edge" systems.[16] Among the applications in the second category are a computer-based drug information system,[17] automatic discharge summary systems,[18] and a computer assisted system for the management of hospital waiting lists.[19]

Probably the best-known leading-edge system is the London Hospital Project. The London Hospital is a multi-facility acute general hospital that serves a large local population in the East End of London; it is also a highly respected teaching institution.[20] The project was launched in April 1968, and by early 1972 the first application was ready to begin, using Univac equipment.

The first application implemented was the waiting list, followed by admission and discharge procedures. A patient index now covers 30,000 records and there is a facility for searching the index with a minimum of identifying data. Additions to the admissions/discharge procedures include a survey of empty beds. "The principal services that have been added, however, are those concerned with requesting laboratory tests--micro-biology was the first, followed by haematology, bacteriology and biochemistry."[21]

Currently under development is an extension of the Patient Index to cover all new outpatients, X-ray requesting and reporting, nursing manpower reporting, and a number of minor applications. These developments require further extension of the communications hardware into new departments of the hospital and an increase in the number of visual display units, printers, and lines from the computer room throughout the hospital.

In May 1970, the Government appointed a Committee on Privacy headed by the Rt. Hon. Kenneth Younger to consider whether legislation was necessary to provide Britons with protection from invasions of privacy arising from activities of private persons and organizations. (The Younger Committee was not given authority to investigate government invasions of privacy. That was to be handled through an "in-house" inquiry by the Government itself, under the Home Office.)

In the area of medical privacy, the Younger Committee considered problems raised by epidemiological research, (such as the terms under which it is permissible for medical research workers to gain access to medical data without the patient's explicit consent) and privacy issues created when individuals were treated by physicians hired by their employers.[22] On the basis of a national opinion survey, the Committee concluded that the British public is not extremely concerned with violations of medical privacy and that the principal dangers stem from the increased access to medical information by non-medical personnel--such as social workers and researchers.[23]

According to the Department of Health and Social Security, the existing status of confidentiality for medical records can be summarized as follows: "The basic principle applied in England to all information obtained or compiled about patients for the purposes of health care is that it will not be used for any purpose other than that for which it was supplied or obtained without the consent of the doctor or dentist concerned and, usually, of the patient. This applies both to personal details provided by the patient himself... and to information compiled by doctors and others relating to the patient's health....Confidentiality is safe-guarded both by the ethics of the medical profession and of those other professions which contribute to health care.

"It is for the doctor or dentist concerned to decide initially whether information about his patient, provided or obtained in confidence, should be disclosed voluntarily outside the health care team; to a relative or a patient, to the patient himself, or to any other person or agency. Medical ethics would usually require that the consent of the patient should be obtained to such a disclosure, but the doctor or dentist concerned would decide whether, in a particular case, disclosure without the express consent of the patient was ethically acceptable....A patient has no right of access to his own personal health records, or to any information contained therein. It is at the discretion of the doctor or dentist concerned to disclose to his patient such clinical information as he considers necessary and advisable in the circumstances."[24]

The code of medical ethics of the British Medical Association states that the "responsibility of a doctor for the safe custody of his confidential records is the same whether the records are conventional or kept in a computer."[25] A 1969 report issued by a BMA Working Party on Computers in Medicine discusses the complexities added to the confidentiality issue by the computerization of health data and notes the need for appropriate procedures to protect the validity and confidentiality of the information.[26]

General concern has been expressed in Great Britain regarding the growing field of medical record linkage. Several groups of doctors protested against the establishment of a central databank for the Oxford Record Linkage Study on the grounds that existing laws and procedures do not afford the records sufficient protection (e.g., the records are not immune to subpoena) and that these records could be linked with social service and criminal records to create general dossiers on persons under government inquiry. Similar objections were made to the establishment of the Mental Health Enquiry, a national psychiatric file. Both of these activities proceeded with their work, however.[27]

In the courts, questions frequently arise concerning the release of medical data, usually in connection with a legal proceeding. In these cases, the courts generally allow the information to be given only to the concerned party's medical advisor, not to the individual or his or her legal representative.[28] Another recent decision requires doctors to give police officers information about a patient which may lead to the identification of a driver alleged to be guilty of a motoring offence.[29]

In December 1975, a White Paper issued by the Government proposed legislation to establish a statutory Data Protection Authority with powers to ensure that computers are used with a proper regard for privacy and with safeguards for the personal information they contain. The White Paper states that the existence and purpose of information systems holding personal data in computers should be publicly known, as should the categories of data they handle, what they do with the data, and who is likely to have access to it. The information should not be used for a purpose other than the one for which it was given or obtained without either the consent of the person whom it concerns, or some other authorized justification. The subject should be able to discover what has been done with the data and to whom it was given, and information should be kept only for as long as it is needed. A temporary Data Protection Authority was appointed to work on the problem during the time period prior to the enactment of the national legislation.[30]

Canada

Primary responsibility for health care in Canada is vested in the provinces, under the administration of a provincial Department of Public Health. Health care services are provided through provincial health insurance programs which cover approximately 99 percent of the population. The federal government supplies half the funding for these programs, while the provinces finance their portion half through general tax revenues and half through monthly premiums paid by families according to their income level.[31] Private insurance companies offer supplementary coverage for items not included in the government plans, such as private beds and the ten percent surcharge that physicians sometimes add.

Estimates of the proportion of the Canadian GNP devoted to health services vary from four percent[32] to over seven percent.[33] In 1971 there were 32,625 physicians in the country, a ratio of one to 661 persons. Nurses numbered 114,303, a 1/186 ratio and there were 7,664 dentists, a ratio of 1/2814.[34] Canadian physicians are paid on a "fee for service" basis, with reimbursement fairly automatic.

The types of automated medical information systems and computer applications in medicine in Canada cover a broad spectrum. One sophisticated system is the Maritime Ambulatory Record System, a federally funded health research project in the Maritime Provinces whose prime objective is the development and implementation of a quality care ambulatory health record system, and the introduction of the system, where appropriate, into private doctors' offices.

At present the Project is using a CRT terminal to abstract information from the patient's record and place it in a computer file, using a Control Data Corporation (CDC) computer. Some outputs that are possible with this system are individual health profiles, family profiles, practice profiles, immunization status report and automatic recall, peer review, and a variety of family medicine research projects. Several factors which facilitate the implementation of such a computerized system in this location are that every resident of the provinces is registered with an insurance number, providing a standard life-long identification; that Medical Services Incorporated, the third party insuror, maintains a population file listing medical encounters for accounting purposes; and that the region is geographically small and discrete, with a population of stable and manageable proportions.[35]

The Department of National Health and Welfare is planning a computerized health record system for the 35,000 people in the Northwest Territories, which will give district health offices access to an Ottawa service bureau through telecommunication links. The system would contain information on individual health, doctors, facilities, and social problems such as alcoholism and drug addiction.[36]

Other types of computer applications in Canadian health care delivery include clinical laboratory systems, which have proved to be cost-effective for high-volume laboratories; a few patient scheduling projects; automated electrocardiogram analysis; multiphasic screening; and medical auditing.[37] At MacMaster University, electronic data processing is used for an epidemiological analysis of patients attending the family practice unit, and registries have been developed for cancer, dialysis equipment, and patients with severe kidney disorders.[38]

The Science Council of Canada recently issued a report recommending the development of regional computerized health information systems covering all Canadian citizens, with the information available to doctors and medical researchers throughout the country. The report found the use of computer-based information processing in health care systems desirable as well as inevitable, and urged the development of health information systems as an essential tool in solving operational and research problems of Canadian health care.[39]

The earliest legislative activity reflecting a concern for privacy protection in Canada came at the Provincial level. In 1968, British Columbia passed a Privacy Act using broad language to prohibit violations of privacy that are willful and "without claim of right." Manitoba passed similar legislation in 1970, and other provinces have concentrated on specific areas of protection, such as consumer credit investigation and reporting.[40]

At the Federal level, the Departments of Communications and Justice commissioned an extensive study on the subject of computers and privacy early in 1971. This report, issued in 1973, noted the absence of legislation assuring the privacy of health data, and pointed out the special problems raised in Canada by the fact that significant amounts of computerized data are actually physically located in the United States. In the medical field, this includes information collected for utilization review, such as Canadian hospitals participating in the PAS data system.[41]

The study found a considerable exchange of health information among government and private agencies. The response to one questionnaire indicated that 78 percent of responding law enforcement agencies, 91 percent of the insurance agencies, 59 percent of oil companies, and 70 percent of the major industrial employers obtain information about individuals from "medical sources" at least some of the time.[42]

In regard to computerized information systems in general, the report commented on the need for regulation of databanks that contain sensitive information about identifiable individuals, with particular attention to accuracy, relevance, control over distribution, security standards, the provision of opportunities for access, and guidelines for collection procedures.[43] The report also concluded that the government, "as the principal collector and instigator of the collection of personal information, has a key role to play," and suggested that some appropriate responses might be the establishment of a surveillance agency and an ombudsman, a code of ethics governing research conducted with government funds, and the implementation of administrative rules enforced by a central agency.[44]

Peter Robinson, deputy chairman of the computer-communications secretariat of the Canadian Federal Communications Department, noted that the creation of the medical databank suggested by the Science Council would require the use of a Single Identity Number to allow doctors and researchers to coordinate information from different sources. He criticized the Council's report for ignoring the issue of privacy invasion that would be raised by adoption of such a number.[45]

As in the United States, the medical record in Canada is considered to be legally the property of the physician, and the hospital record belongs to the hospital.[46] While the question of patient access to records is a looming issue, privacy and confidentiality problems have so far received more attention.

A proposed piece of legislation in Canada, the Canadian Human Rights Act, is partially devoted to the protection of personal information, and if passed would affect government-held medical records. The Act would permit the Government to issue regulations prescribing the conditions under which third parties would have access to identified records, when individuals would be notified that records are maintained about them, and under what circumstances records could be corrected.[47] The bill has passed only its first reading, with the remaining two readings not expected soon.[48]

Federal Republic of Germany

The Federal Republic of Germany has one of the oldest public health insurance programs in Europe, dating back to 1883. Presently over 90 percent of the population is insured through statutory programs. Other forms of protection, such as private insurance, bring the percentage of persons covered by some form of health insurance to 98.6 percent.[49]

The administration of the system is decentralized, with 1,800 local health insurance "funds" serving the population. There are three general categories of persons covered by the statutory program. Those compulsorily insured consist of all wage earners, salaried employees with incomes below a prescribed ceiling, and persons receiving unemployment benefits or assistance; 59% of insured persons are in this group. Age-old pensioners comprise a second group, and account for 26 percent of the insured population. Finally, 15 percent are voluntarily insured, and consist of self-employed persons with incomes below the ceiling, salaried employees not formerly insured, new entrants into employment at a salary above the limit for compulsory insurance, and various groups undergoing occupational training.[50]

Financing of the health insurance plans is generally through contributions from employers and employees, with the fee schedule determined by income levels. Direct contributions by the government are minimal, although there are several indirect methods of government assistance, such as subsidies to the compensation funds of small companies and direct allocations to health providers.[51]

Normally doctors are remunerated on a fee-for-service basis. The physicians report the services rendered to the local practitioners' association, which presents the claims to the sickness funds and distributes the payments due.[52]

The physician/population ratio in West Germany is fairly high, better than one per 600 persons in 1973.[53] In 1965 there were 14.5 doctors for every 10,000 people, as compared to 11.7 in Canada, and 11.5 in the United Kingdom.[54] A 1969 estimate indicated that 5.7 percent of the German GNP was expended on health services.[55]

There were 3,601 hospitals in the Federal Republic of Germany in 1969, with an average of 188.2 beds per hospital. Public hospitals numbered 1,345; private charitable institutions 1,281; and there were 975 private profit-making hospitals.[56] The number of hospital beds per 10,000 population in 1965 was 107; in Canada it was 110, in the United Kingdom 105.5, and the United States 90.[57]

A leading-edge German computer system is the Medical System Hannover (MSH) at the Hannover Medical School Hospital, an independent medical school owned and operated by the State of Lower Saxony.[58] A major objective of the project is to "provide a system for the acquisition, integration, retrieval, and analysis of information about hospital patients and hospital resources in order to support patient and hospital management, and to provide data for scientific analysis.[59]

The system operates a central databank with files on both magnetic disc and tape storage. A Status Summary File contains information for all patients who have ever been admitted, and the system keeps condensed relevant information on-line as long as possible. Every Hannover patient is given a unique ten-digit identification number, assembled from the birth date, birth name, sex, and a running counter. This number is the ordering and search key for the system. Several administrative functions are performed by the MSH, including admissions and billing, and a pharmacy system is under development.

The computerized data base has not replaced the manual chart; that is used during the patient's stay and then microfilmed, with the paper record destroyed after the patient's discharge. Although the computerized system does not yet contain sufficient data to be comprehensive, its contents is growing rapidly and Hannover hopes to extend it to a complete record.

Although less concern for the problems of data collection and privacy has been voiced by the public in Germany than in some other industrialized nations, the issue of data protection did become more prominent in the late 1960's with the institution of computerized population registries and a government plan to introduce a uniform national personal identifier.[60]

Several West German states (länder) pioneered in creating administrative protections for personal data in computer systems. The Data Protection Act of the State of Hesse, passed in 1970, was the first such general statute enacted in a Western nation. The Act applies to all public automated data systems under the jurisdiction of the State of Hesse, and its objective is to insure that data shall be obtained, transmitted and stored in such a way that it cannot be used, altered, or destroyed by unauthorized persons. Persons responsible for the preparation, transmission, storage or automatic processing of data must adhere to strict standards of confidentiality, and individuals have the right to correct inaccurate data about themselves.[61]

A significant feature of the Act is the creation of an Office of Data Protection Commissioner. This person functions as an ombudsman to receive complaints from the public and is also directed to insure compliance with the 1970 act and other regulations concerning confidential handling of personal information. The Commissioner can also set additional measures to improve data protection.[62]

Other West German states have since passed similar legislation. There have also been several attempts to enact a Federal law, the most recent draft of which is a currently pending Data Protection Act introduced by the Ministry of the Interior. This bill would cover both manual and automated data systems, in the public and private sectors. However, different regulations would be applied to public databanks, data processing by private organizations for internal purposes, and data processing done for third parties by private agencies on a professional basis, such as credit agencies and publishers of mailing lists.

The rules for the first two categories are quite general, with no provision for an independent supervisory institution that could make the broad provisions of the Act more specific and supervise administrative compliance. Only in the last category - service bureau operations - is there a provision for outside control, but this is through supervisors at the state rather than federal level. One important requirement is that an individual be notified the first time data concerning him or her is communicated.[63]

As in most Western European nations, the Federal Republic of Germany has a broad declaration of the doctor's duty to remain silent on confidential information concerning a patient, (paragraph 300, Deutsche Strafgesetzbuch).[64] There is no specific legal ban on the use of medical information for secondary purposes.

Australia

In 1975 Australia passed legislation which replaced its voluntary health insurance system with a compulsory tax-financed system known as Medibank.[65] Before that, about 78 percent of the population (a 1972 figure) had been insured for medical benefits and 80 percent for hospital benefits.[66] Under the current system, medical services continue to be provided predominantly by private practitioners on a fee-for-service basis, but a single Governmental Health Insurance Commission now provides reimbursements.

Privacy issues have received increased attention in Australia in the past few years. The Labor Party included in its 1973 national platform a commitment to "the right of privacy."[67] There has also been debate recently on whether Australia's accession to the United Nations International Covenant on Civil and Political Rights (which repudiates "unlawful interference with...privacy" and establishes the right to protection of law against such interference) will raise protection of privacy in Australia from a State to a Federal issue, as a matter of treaty obligation.[68]

The Jaycees of New South Wales issued a widely quoted report in 1968, "Invasion of Personal Privacy," which explored such issues as surveillance and the credit industry. In 1975, the State of New South Wales established a Privacy Committee to research and develop a general policy towards privacy. It is to receive, investigate and mediate in complaints by individuals regarding unjustifiable invasions of privacy; to disseminate public information and stimulate public debate on the issues; and to recommend law reform and changes in administrative and business practice.[69]

Currently the only laws at either the State or Federal level protecting the confidentiality of medical records are statutes in the Evidence Acts of the States of Victoria and Tasmania prohibiting physicians from testifying about patients in legal proceedings without their consent.[70] In Victoria, this privilege has been interpreted by the courts as also applying to the provision of written documents.[71]

When the national health insurance system was being debated in 1973-74, the problem of protecting the confidentiality of medical records became the target of sharpened concern. The Australian Medical Association based part of its objection to this program on the absence of privacy safeguards in the legislation. In 1973, the Attorney General established a Committee of Enquiry into the Protection of Privacy, to recommend legislation to protect individual privacy under the proposed health insurance arrangements.[72]

In December 1973, the Committee issued a report with recommendations concerning the collection and retention of information by the Health Insurance Commission, the confidentiality of health data, individual rights of access, and the security of health information systems under Medibank. However, this report was tabled in both houses of the Australian Parliament in 1974.[73] Medibank thus went into effect on July 1, 1975 without statutory safeguards for privacy.

A Bill was then introduced into the Federal Parliament to amend the Health Insurance Act by incorporating provisions to protect the privacy of individuals, as recommended by the Committee. Among these provisions are requirements which would restrict access to medical records to persons requiring such access for operation of the program, establish a record of every access to a record that is not a routine access essential to daily operation of the Health Information Act, allow individuals access to their own records, and destroy records after a specified time period. The Bill would also require persons with access to medical records to protect the confidentiality of the data and require the issuance of a warrant in order for police to have access to medical records.

Due to the dissolution of the Australian Parliament in November 1975, the Bill lapsed. However, the new government is expected to introduce similar legislation at the 1976 parliamentary session.

Currently, Medibank patients are identified by a unique numbering system; although the number is based on personal details, such as birthdate, it is coded so that this information cannot be determined from the number. It is not necessary to produce a Medibank card or to quote a Medibank number to obtain medical services, if identity can be proved by other means. It is also possible to claim Medibank benefits without quoting the Medibank number if the required personal details are given.[75]

Patients' claims histories are automated, with access by means of the Medibank number only. History printouts contain number but not name. Requests for printouts are monitored by a security officer in each processing center, who ensures their destruction after use. Documents and microfilm copies of documents are not held in claimant or patient files, but are filed in order of processing which makes unauthorized access difficult.[76]

One other event which stimulated discussion about privacy of medical records was a Seminar on Medical Records Systems in Primary Health Care, held in Canberra in April 1974 by the Hospitals and Health Services Commission and the Royal Australian College of General Practitioners. The recommendations which resulted from this Seminar emphasized the need for detailed, integrated health records and the importance of protecting the patient's privacy while meeting the needs of practitioners, administrators, and researchers.

France

Over 99 percent of the French population is covered by compulsory health insurance, either through the general national plan or special plans for groups such as miners, agricultural workers, seamen, civil servants and railway employees. However, coverage under these programs is not complete, so that additional insurance and private incomes also finance a significant proportion of French health care.[77]

Most of the industrial work force is covered by the general scheme administered by the National Sickness Insurance Fund, which is directly supervised by the Ministry of Public Health and Social Security and the Ministry of Finance. The Fund in turn supervises 16 Regional and 121 Primary Sickness Insurance Funds. Local branches of the sickness funds are financed from the central general fund and are the agencies which provide cash refunds to individual health care customers.[78]

Many benefits cover only part of the cost of medical care in France; for example, the insurance fund usually repays the patient for medical expenses at the rate of 75 percent of the cost based on the current scale of fees in the locality where the nearest doctor to the insured's home resides. As a consequence, 61.4 percent of the French population belong to mutual societies to augment their coverage.[79]

The Benefits system administered by the National Sickness Insurance Fund is financed by contributions made by the employer and employees. Contributions are based primarily on earnings, with the employer bearing most of the costs.[80]

In 1971, approximately 5.5 percent of the French GNP was spent on medical care.[81] The ratio of physicians in the population as of 1968 was 12.8 per 10,000, with great regional variation. Similarly, there were 214 nurses and 518 hospital beds per 10,000 population. The total number of doctors in France in 1972 was 68,778, a ratio of 1.335 per 1,000 population. Of these, almost 50,000 were treating private patients during at least part of their working year.[82]

For many years, any protection of privacy under French law rested on the generalized command of Article 1382 of the Civil Code of 1804. This states, "Any act which causes injury to another renders the person responsible for the act legally bound to repair the injury." Specific provisions added to this law over the years dealt mostly with the duties of lawyers, physicians, public officials and other similar persons to preserve the confidentiality of personal information revealed to them in the course of their occupations.[83]

A new provision dealing expressly with privacy was inserted into the Civil Code in 1970. It provides: "Everyone has the right to have his private life respected. Judges have the power...to prescribe all measures...which may be necessary to prevent or stop an intrusion on or into the intimacy of private life...." This statute is far less powerful in practice than it seems on its face, however, because it is difficult to define in a particular case whether an action does constitute such an intrusion.[84]

Currently, the legal basis of medical secrecy is found in Article 378 of the Penal Code, which states: "Physicians, surgeons and other health officers, together with pharmacists, midwives, and all others who by reason of profession...are entrusted with secrets confided to them, except where obliged or authorized by law to give testimony, having revealed these secrets, shall be punished by imprisonment of from one to six months and to a fine of 500 to 3,000 francs.[85]

This rule of secrecy is not absolute, as the patient may lift it. Physicians are also obligated to report certain medical facts to public services, e.g., contagious and occupational diseases, and medical records may be required for a legal proceeding. Another factor complicating rules of medical secrecy and access in France is that, according to 1970 and 1972 decisions by the French Supreme Court and Council of State, the files in a medical center belong to the center itself and not to the physicians who assembled them; therefore only the doctors currently in practice at the center may see them, and the originating physicians may not.[86]

In 1974, there was considerable furor in France over reports that a government project, code-named "Safari," was under way to give every person in France a single identification code, in order to facilitate the quick retrieval of information stored by different data systems. As a result of public outcry, the Government appointed the Commission Informatique et Libertés (Commission on Automation and Liberty). The Commission, headed by Bernard Chenot, vice president of the Council of State, held extensive hearings and did studies of the databanks and privacy issue in the main sectors of record-keeping about French citizens.

Its report, issued in September, 1975, notes the dangers in the growth of data systems, both manual and automated, and points out that even without a single identifier it is possible to match files through common elements. The report suggests that individuals need to check the veracity of data in files concerning them and that they should be able to correct errors and fill gaps. The report also recommends the creation of a standing committee on data systems and liberty "responsible for supervising the negative and positive regulations pertaining to data processing."[87]

A Health Committee of the Chenot Commission submitted a background Report on Medical Files to the main Commission, after studying files containing medical information maintained by all organizations coming under the jurisdiction of the Ministry of Health. These files fall into three categories: 1) Hospital Logistics files--28 systems which are essentially administrative, with only minor content of medical information; 2) Medical Methodology Systems--258 systems which process medical information with the goal of improved therapeutics, or analyze data from analytical or diagnostic equipment, or do epidemiological statistics; and 3) Medical Dossiers--81 systems usually used for processing partial medical records associated with one disease treated by a particular hospital.

In terms of their potential risks to individual rights, the Health Committee found that those in the first category, although primarily administrative, still contain sensitive personal information and need protection. The second type, automated medical systems, are mainly impersonal, but could be sensitive in an interconnected network of systems. The medical dossiers always contain personal medical histories, and are therefore always susceptible to rights violations.

The main report offered a series of suggestions to cope with threats to individual rights caused by data systems, including several related specifically to medical records: 1) the creation of a permanent board to serve as a source of information, advice, and advocacy in matters concerning automation and civil liberties; 2) a review of the judicial basis of medical secrecy; 3) the binding to secrecy of the holder of a medical file; 4) publication of the existence of medical file systems and the identity of the persons responsible; 5) the prohibition of certain uses of medical files, with the clear indication of the purpose of a system at the time of installation; 6) the authorization of certain files only after investigation by a supervisory authority; 7) the design of files so that patients are not excluded from information that others may share; and 8) a system for data verification by the patient or by an independent second opinion with access to the same information from which the file was created.[88] These proposals are now before the French Parliament.

Sweden

All resident Swedish citizens are covered by compulsory health insurance. Prior to 1955, voluntary health insurance was provided by a network of registered sickness funds; since 1963, a comprehensive national insurance program has been in effect. This system is administered by 26 regional insurance offices; these are regarded as independent but operate under the central supervision of the National Social Insurance Board. This Board is responsible to the Minister of Health and Social Affairs.[89]

Swedish residents may enter the state health system through any one of three avenues: hospital out-patient departments, which account for half of all ambulatory consultations; district medical officers, who account for 25 percent of ambulatory care; and private practitioners, in which case the patient pays the doctor's fee and is reimbursed by the insurance office for 75 percent of the appropriate amount on a sickness-insurance tariff fixed by the Government. Hospitalization is free to the patient.[90]

Financing of this system is also tripartite. The State subsidy covers 55 percent of all medical benefit costs other than drugs. The employee contribution is a combination of flat rate and percentage of income, and the employer's contribution is a percentage of payroll earnings. (Self-employed persons also make a contribution.) Hospitals, the district medical officer service, and supporting local health services are provided at the county and municipal level out of local taxation.[91]

The number of active medical practitioners in Sweden in 1970 was 10,500, or one per 760 population. Hospital physicians form the large majority of doctors; they are salaried, as are district medical officers. More than 3,000 doctors are engaged in private practice, either totally or in off-duty periods. At the end of 1970, there were 130,000 hospital beds in Sweden, a ratio approaching 17 per thousand population. All beds in public hospitals are public; unlike several other European countries, it is not possible to pay extra for more private facilities in such hospitals. While there is little private health insurance in Sweden for medical costs, there is insurance to provide cash income during illness.[92] In 1971, 8 percent of the Swedish GNP was devoted to health care.[93]

Sweden is the site of several advanced medical information systems. One of these is the Stockholm County Medical Information System, at Danderyd Hospital. This is administered by the Stockholm County Medical Service Board, which serves a population of 1.5 million persons and has under its jurisdiction 71 hospitals with 20,700 beds.[94] When the Stockholm County Council decided to implement this system in 1967, its requirements were that the system 1) cover the entire county; 2) be "real time;" 3) be modularly designed so functional routines could be added progressively; and 4) cover routine administrative as well as medical and planning functions.[95]

Since each Swedish citizen is assigned at birth a ten-digit identification number, containing his or her birth date, this number was chosen as the patient identification number for the system. This made it easy to obtain initial personal identification information for the system from census and tax files. A Univac computer was installed at Danderyd in 1968 and a second one was added in 1971. The system is designed to handle the flow of information between individual physicians, medical departments, and hospitals throughout the region.

There are three primary files in the system. The Main File (on-line) contains medical information on all in-patient visits and X-ray examinations performed in the county since the beginning of 1968. The file, comprised of relevant data on all "presumptive patients," meaning all inhabitants of the county, includes Census information, critical medical information, information on previous in-patient care, and information on previous X-ray examinations. The file is updated weekly from magnetic tapes from the Central Population Registry.

An on-line Patient File for each hospital or group of hospitals contains information on current patients. This data is stored only during the time the person is actually a patient. A Medical Records File, containing all information from previous and current treatment periods, is presently still stored manually. Within two years, such medical records will be stored on microfilm. In addition to these main patient files, there are Health Controls and Home Care Files which contain information on examinations and tests to be performed, on results of tests and analysis, and on ordered therapies. A Statistics File contains selected information from the patient files and from health care systems and is processed in batch mode.[96]

Among the functions performed by this system are information retrieval from the main population file, in-patient registration, resource scheduling and booking, out-patient registration, laboratory routines and waiting list. The system is in operation 24 hours a day, with about 300 terminals in operation.

In 1970, when the Swedish public began to be concerned about issues of privacy and technology, the most important relevant statute was the national Secrecy Act. This law exempts from disclosure to the public and the press certain categories of records, such as those dealing with foreign affairs, the questions and results of competitive examinations, and depositions and evidence in court cases that have not yet come to trial. For other classes of records, such as census and tax-return records, the Act restricts circulation whenever the subject of the record has not given express permission for its further use. The Act also provides that personal records of medical care, social rehabilitation aid, financial status, family affairs, and the like, should not be revealed.[97]

With the publication of the 1970 census, an intense and unexpected controversy over privacy arose within Sweden. This stemmed from growing public uneasiness over computerizing the census and other related statistical activities that used personal identifiers. The two main points raised during this debate were 1) collecting data about people, their attitudes, and their life-styles could give the authorities a possibility of too much of control over the affairs of individuals; and 2) the expansion of automated data processing seemed to presage a super-efficient, unforgiving police state, very different from the customary paternalistic bureaucracy to which Swedes were accustomed.

The task of examining the effects of automatic data processing on traditional record-keeping laws and practices was given to an advisory committee in the Justice Department that was already at work on the broader problem of recodifying the Freedom of the Press Act. During 1970 and 1971, the Committee on Public Access and Secrecy surveyed the use of automatic data processing in both the public and the private sectors. In its 1972 report, the Committee found that although public unrest about wide-spread intrusion upon personal privacy was not objectively supported by the evidence, the growing use of the computer in gathering, storing, processing and disseminating information about people was introducing sufficient changes in the nature and power of administration so that new legal measures of control were needed.

The Committee presented draft legislation designed to regulate the effects of computerized record keeping while allowing the rationalization that automatic data processing is capable of bringing to complex administration.

The Swedish Data Act was passed substantially as drafted and became law on July 1, 1973, to take effect on July 1, 1974.

Under the Act, every business or government agency wishing to maintain a computerized file of information containing data which can be identified with a particular individual must first obtain the permission of the Data Inspectorate, a nine-member public body appointed by the King-in-Council. The Data Inspectorate grants permission to operate a personal file system if it finds there is no reason to expect it to create undue risk of intrusion into the privacy of the persons registered. No licensed system may store medical or criminal-record data unless it is authorized to do so by law or this has been specifically approved by the Data Inspectorate.

The Act defines with considerable precision the duties of the "responsible keeper" of each registered file. He is liable for criminal penalties provided for violation of the Act. The responsible keeper must furnish any data subject, upon request, with a complete copy of all information about him or her contained in the file, unless--as with certain medical and criminal data--that is expressly prohibited. If the personal data are found to be incorrect, the keeper is obliged to have them corrected; if incorrect data have been disseminated by the system, the recipients must be notified of the corrections.

The Data Inspectorate, in addition to acting as a national licensing body, is also responsible for supervising and inspecting registered systems, as well as serving an ombudsman (citizen complaint) function for all government data-processing activities.

Because the Data Law of 1973 and Swedish automated medical record systems developed side by side, an equilibrium was established from the early 1970's onward between the goals of the medical record keepers and the requirements of the law. Therefore, passage of the Act caused little fundamental change in medical record keeping.

Decisions of the Data Inspectorate on licenses for new automated medical systems have established several main points. First, the information that is usually kept in typical medical records may be automated unless the amount of information is so extensive that it constitutes a comprehensive description of an individual. In such a case, the personnel who have access to the system must be sworn to secrecy, and breaching that duty carries criminal penalties. Second, information collected especially for a medical system must be given by the patient under a clear understanding of the purpose and scope of the system. Third, statistics produced by the system must not disclose any information about an identifiable individual. Fourth, the system must be used only for the purpose stated in the application, and only the approved data and processing steps may be used. Fifth, systems used in support of a particular research project must be purged when the project ends, and the permission granted by the Data Inspectorate in such instances is valid only for a stated period.

In cases where a medical system raises unusual problems due to the sensitivity of the information, the Data Inspectorate has not hesitated to mandate stronger safeguards. For example, where a research project to evaluate the success of an alcohol clinic would gather much of its data through personal interviews with the patients, the Inspectorate set especially thorough requirements for informed consent.

According to the Data Inspectorate, the most sensitive aspects of medical records so far have involved political questions connected with maintenance of the immigrant children's medical register, and legal issues connected with a narcotics register. In the latter case, the Inspectorate is aware that police do get information from automated systems on occasion, even though this is not permitted; since this police access has been infrequent, on a verbal basis, and accomplished through the cooperation of narcotics register employees with authorized access, the Data Inspectorate does not feel that this problem can be solved by altering the conditions of automated files, but requires strengthening the supervision of register employees.

SUMMARY

Looking at the overall patterns of computer use in health care in other democratic nations, we can draw the following conclusions:

(1) computer use in Europe and other industrial democracies is still heavily centered on administrative and laboratory applications for hospitals, and administrative and claims-processing operations for health insurance purposes;

(2) leading-edge hospital systems are still experimenting with their work on automated patient records and patient information systems;

(3) only a small number of clinics and hospitals in various nations are working, slowly, toward a unified hospital information system;

(4) there are only a few working models of regional health information systems;

(5) problems of cost-justification, organizational and medical opposition to technological innovation, and competition between medical and social priorities for money and management attention are part of the basic scene in all these nations; and

(6) national health information systems for planning and public health purposes are still in their infancy.

In short, while computers have aided in administrative aspects of health care, and have made some valuable contributions to direct patient services in other nations, the fundamental problems that have impeded greater use of and greater payoff from computers in American health care have been duplicated in other nations, and remain the issues confronting all health system planners today.

As far as protection of citizens rights in medical data, and especially in new automated data systems, there are several models of legal protection emerging among the industrialized democracies, paralleling the way such nations are dealing with the larger records-and-privacy issue in their societies. In terms of what has already been adopted, one model is represented by the Swedish Data Act and similar regulation at the West German state level. Here, automated personal data systems are being officially licensed, with detailed regulation and continuing oversight assigned to administrative boards or commissioners. Medical data systems in these countries represent one type of system covered by the general protective scheme, so that the definitions of privacy, confidentiality, and individual access, and the safeguards required in such systems are being worked out by the regulatory authorities as initial licensing, practical experience, and citizen complaints develop.

In most other industrialized democracies, national legislation to protect privacy has been recommended by parliamentary or special commissions and is currently under legislative consideration, with adoption of various schemes reflecting different national political cultures virtually certain by the end of the 1970's. In some of these nations, specific safeguards for national health insurance data or data kept by primary care providers have been recommended, as in Australia, and such measures will probably be adopted separately.

What is especially worth noting in this situation is the widespread agreement in parliamentary democracies on the principles of citizen rights in record systems that need to be observed, whatever regulatory mechanisms may be chosen to enforce them. There is general consensus that data systems should be limited to the information necessary and relevant for the function being performed; that data systems should not be secret; that individuals should have appropriate notice of the records kept about them and of those who will have access to the information; and that procedures should be provided to allow individuals to inspect their records and assure their accuracy and completeness. As to the special regulations needed for computer systems, the British White Paper of 1975 expressed what a decade of alarms, studies, and public debates has now made a common outlook in Western nations:

"The time has come when those who use computers to handle personal information, however responsible they are, can no longer remain the sole judges of whether their own systems adequately safeguard privacy. The safeguards must become subject to independent scrutiny."

FOOTNOTES

1. For a report on these trends as of 1973, see Alan F. Westin, David B.H. Martin and Daniel H. Lufkin, *The Impact of Computer-Based Information Systems on Citizen Liberties in the Advanced Industrial Nations*, Washington, German Marshall Fund, 1973.
2. Presentation of these themes can be found in the papers for sessions 2.2 ("Experience with Computer-Based Medical Information Systems") and 2.3 ("Improving Health Care Delivery in the Community") in *Medinfo* 74, First World Conference on Medical Informatics, 1974.
3. Derick Fulcher, *Medical Care Systems*, Geneva, International Labour Office, 1974, pp. 88-89
4. *Ibid.*, pp. 93-95.
5. Alan Maynard, *Health Care in the European Community*, Pittsburgh, University of Pittsburgh Press, 1975, p. 192; and Fulcher, p.88.
6. Maynard, p. 193.
7. *Ibid.*, pp. 188-91.
8. *Ibid.*, p. 196.
9. *Ibid.*, pp. 200-201.
10. Fulcher, p. 93.
11. Maynard, pp. 205-206.
12. *Ibid.*
13. *Ibid.*, p. 95.
14. Harry Orriss, "The National Health Scene," *Computer Weekly*, January 2, 1975, p. 23; and J. Sharpe, "Towards a Methodology for Evaluating New Uses for Computers," *Medinfo* 74, pp. 137-43.
15. B. Barber, "The Place of the Computer in the Delivery of Health Care," in *Computer Information Systems in Health Care*, London, Sperry Univac, 1975, p.9.
16. W.C. Abbott, "The London Hospital Project," Seminar on Computer Applications in the Field of Medicine, Sperry Univac International Executive Centre, Rome, November 25-27, 1975.
17. C.R. Henney, P. Brodile, and J. Crooks, "The Administration of Drugs in Hospital--How a Computer Can Be Used To Improve The Quality of Patient Care," *Medinfo* 74, p. 271.
18. P.J. Dixon, "Communications Between Hospitals and Family Doctors," *Medinfo* 74, pp. 539-41.
19. T.C.S. Kennedy and N.B. Moss, "A Computer Assisted Clerical System for Management of Hospital Waiting Lists," *Medinfo* 74, p. 497.
20. This discussion is based on Abbott, *op. cit.*, and W.C. Abbott, "Planning and Implementation of the London Hospital Project," in *Computer Information Systems in Health Care*, pp. 19-25.
21. Abbott, "The London Hospital Project."
22. Report of the Committee on Privacy, London, Her Majesty's Stationery Office, 1972, pp. 110-15.
23. *Ibid.*, pp. 113-14.
24. Communication to Medical Records Project from Department of Health and Social Security, London, December 11, 1975.
25. British Medical Association Members Handbook, p. 17.
26. *Computers in Medicine*, Planning Unit Report No.3, London, British Medical Association, 1969.
27. Joseph Hanlon, "U.K. Doctors Protest Government's Medical Data Banks," *Computerworld*, November 14, 1974.

28. "Disclosure of Medical Reports Limited to Doctors," London *Times*, May 15, 1974; and "Disclosure of Hospital Records," London *Times*, October 25, 1974.

29. "Law Report: Doctors Must Tell the Police," London *Times*, February 9, 1974.

30. Peter Evans, "Plan to Ensure That Computers Have a Regard for Privacy," *The London Times*, December 17, 1975, p.4.

31. Canadian Computer/Communications Task Force, "Branching Out," Ottawa, Department of Communications, 1972, p. 134; and John R. Evans, M.D., "Health Manpower Problems: The Canadian Experience," in *Manpower for Health Care*, papers presented at National Academy of Sciences, Washington, D.C., May 8-9, 1974, p. 89.

32. Canadian Computer/Communications Task Force, p. 134.

33. Fulcher, p. 93.

34. Evans, P. 91.

35. D.B. Shires et al., "MARS and the Family Doctor," *Medinfo* 74, pp. 277-79.

36. Canada, Department of Communications and Department of Justice Task Force, *Privacy and Computers*, Ottawa, Information Canada, 1972, p. 74.

37. Canadian Computer/Communications Task Force, pp. 147-55.

38. J.M. Carroll, et.al., Personal Records: Procedures Practices and Problems; A Study for the Privacy and Computers Task Force, Ottawa, Department of Communications, Department of Justice, pp. 147-48.

39. T.M. Whiteman, "DP-Based Health Care Crucial, Canadian Science Council Warns," *Computerworld*, January 8, 1975, p. 7; and "Not So Fine and Private a Place...." *Computer Weekly*, November 14, 1974, p. 10.

40. Westin, Martin, and Lufkin.

41, J.M. Carroll et al, p. 159.

42. John M. Carroll, "Assuring Information Protection in the Health Sector," Paris, Seminar on Policy Issues in Data Protection, April 22, 1974, pp. 4-5.

43. Canada, Department of Communications and Department of Justice Task Force, p. 122.

44. *Ibid*., p. 184.

45. "Not So Fine and Private a Place...", note 39.

46. Amy Chouinard, "Shall I Not Ask for Whom the Medical Record is Kept?" *Canadian Medical Association Journal*, February 22, 1975, p. 508.

47. Bill C-72, House of Commons of Canada, 1st Session, 30th Parliament, 1974-75.

48. Communication to Medical Records Project from Project on Privacy and Access to Government Microdata for Social Science Research, University of Western Ontario, London, Canada, November 25, 1975.

49. Fulcher, pp. 69-70.

50. *Ibid.*, pp. 70-71; and Maynard, p. 9.

51. Maynard, pp. 16-21.

52. Fulcher, p. 76.

53. Fulcher, p. 74.

54. D. Stark Murray, *Blueprint for Health*, New York, Shocken Books, 1974, p.33.

55. Fulcher, p. 93.

56. Maynard, p. 38.

57. Murray, p. 33.

58. P. Reichertz, "University of Hannover Hospital Computer System (Hannover)," in Collen, pp. 598-661.

59. *Ibid*.

60. Otto Mallmann, "Computers and Civil Liberties: The Situation in the Federal Republic of Germany," *Law & Computer Technology*, January/February 1974, in United States Senate Committee on Government Operations, *Privacy and Protection of Personal Information in Europe*, Washington, D.C., United States Government Printing Office, March 1975, pp. 90-91.

61. *Ibid*., p. 91.
62. *Ibid*.
63. *Ibid*., pp. 93-94.
64. See Th. Fischer and J.M. Helmbock, "Data Privacy and Data Security in Kiel KIS," *Medinfo* 74, 1974.
65. Communication to Medical Records Project from Australian Medical Association, November 6, 1975.
66. Fulcher, p. 117.
67. *The National Times*, Sydney, 20-25 August, 1973, p.7.
68. Westin, Martin and Lufkin, pp. Australia 4-5.
69. *Privacy*, Newsletter of the New South Wales Privacy Committee, Vol. 1, No.1, October 1975, pp.2-3.
70. Victorian Evidence Act, 1958, S. 28(2); and Tasmanian Evidence Act, 1910, S. 96(2).
71. *Caruci v. Housing Commission*, Supreme Court of Victoria, October 10,1972, in *Victoria Reports*, April 1973, p. 215.
72. Communication from Australian Medical Association, November 6, 1975.
73. Communication to Medical Records Project from Australian Health Insurance Commission, December 12, 1975.
74. Communication to Medical Records Project from W.J. Orme, Executive Member, New South Wales Privacy Committee, November 27, 1975.
75. Communication from Health Insurance Commission, December 12, 1975.
76. *Ibid*.
77. Maynard, pp. 107-108.
78. *Ibid*.
79. *Ibid.*, pp. 112, 127-28.
80. *Ibid*., p. 115.
81. *Ibid.*, p. 127.
82. *Ibid.*, pp. 142-43, 136.
83. Westin, Martin and Lufkin.
84. *Ibid*.
85. G. Brainbant, "Le Secret des Données Medicales," Paris.
86. *Ibid*.
87. Phillippe Boucher, "Keeping Tabs on Citizen Dupont," The *Guardian*, October 4, 1975.
88. *Annex D-2, Rapport de la Commission Informatique et Libertés*, Paris, Documentation Francaise, 1975.
89. Fulcher, pp. 141-43.
90. *Ibid*., pp. 143-44.
91. *Ibid*., pp. 145-46.
92. *Ibid*., pp. 146-49.
93. H. Peterson, "The Stockholm County Medical Information System," in *Computer Information Systems in Health Care*, p. 27.
94. H. Peterson, "A Password Oriented Privacy System for Stockholm County," *Medinfo* 74, p. 645.
95. Peterson, "The Stockholm County Medical Information System," pp.27-28.
96. *Ibid.*, pp. 28-31.
97. Westin, Martin and Lufkin, Sweden, p. 6.

CHAPTER 13: POLICY ANALYSIS AND RECOMMENDATIONS

INTRODUCTION

To set the perspective for our policy analysis and recommendations, three summary observations are important:

1. Medical records and health data are being used today in an enormous variety of settings, with computerization present in all of them. Our report has traced such use in doctors' offices, clinics, health centers, and hospitals; in governmental and private facilities; in acute and ambulatory care; in physical medicine and psychiatric treatment; where patients could choose their health care and where they are under various institutional controls (prisons, the army, mental hospitals, etc.). We have seen that beyond primary care lie important uses of personal medical data for service-payment, quality-care review, and all the social processes we discussed as Zone 3 activities, from credit, employment, and licensing to law enforcement, social research, and political life.

Given this great diversity of settings, there is no single public-policy intervention that can be expected to set standards for the protection of citizen rights throughout the health care system and covering all other health data uses. No constitutional amendment, model statute, judicial rule, systems guide, or managers' code could encompass, by itself, all the important problems that need attention, nor would the actions of any one of these policy-forming authorities be adequate in terms of regulatory scope and supervisory power. Thus our initial assumption is that wise standards will require a mosaic of policies, applied by different authorities and institutions in our social system, hopefully adding up to a consistent national approach.

2. Members of the project team (just as readers of this report) hold differing views about how American health care should be organized, financed, and conducted, as well as on the issue of where computers can and cannot be used to good advantage in the health-care process. But we take it to be a paramount requirement of American society, based on its concern for individual dignity and humane values, that citizen rights should be adequately protected regardless of the health-care or computer-system options that may be pursued in the coming years. To be sure, some models of health care or information-system plans lend themselves more easily than others to the installation of civil liberties guarantees, and there are some systems (current or proposed) that are so potentially violative of citizen rights that they deserve to be opposed entirely. But, as we see it, our objective should be to assure that every institution now collecting or using personal health data observes basic guarantees of individual rights, and that every reform of our health care systems or adoption of new computer applications in this field demonstrate how it will follow similar policies. We cannot allow such issues of citizen rights to become matters for "later consideration," to be seriously addressed only after "more basic issues" of health care are resolved.

3. While the need to protect personal medical data against misuse has been recognized recently by influential voices in the medical, computer, and civil liberties communities, and while we are beginning to apply important new laws such as the federal privacy act, we have still not moved very far to bring health data systems under a set of guiding principles and procedures. To reiterate what we

said in the conclusion to Chapter 11:

> "Most computerized health data systems are being created or expanded without sufficient consultation in advance with groups representing citizen rights and doctor-patient interests, and without some kind of proceeding open to the general public. Most data systems lack sufficiently developed analyses of how much and what kind of identified personal data they really need to perform their function. Even when properly defined, most data systems fail to adopt sufficiently precise standards of confidentiality, controlling uses within the organization and release of identified data to third parties. When it comes to rules for permitting patient access to their own records, very few computerized organizations have adopted procedures responsive to those patients who ask for and insist upon access...What we have today are ambiguous and ill-defined systems that leave people uncertain and fearful about their capacity to control the circulation of their medical and health data."

In short, while we are not without some useful precedents and tools for the job, securing individual rights in the increasingly computerized world of health care is a job that has barely begun.

ELEMENTS OF A NATIONAL POLICY

To evolve a unified national policy, we need to (A) adopt a coherent theoretical approach to the balancing of individual and social interests in the use of data systems; (B) apply these to produce basic principles or standards for the operation of health data systems; and (C) identify some current priorities for policy action in the health area. These will be the major sections of our discussion in this chapter.

A. GENERAL CONCEPTS GOVERNING DATA SYSTEMS IN DEMOCRATIC SOCIETY

Looking over American society's encounters with the privacy-and-databanks issue during the past decade, we see the gradual emergence of a set of basic concepts that command a wide public concensus today, and can be drawn upon with great value in making policy choices in the health field. Since these ideas have been discussed at great length elsewhere,* we will present them only briefly, in the expectation that probing their conceptual strengths and weaknesses, and applying them to real-world situations, will be the work ahead for many years.

---

*See, for example, Westin and Baker, Databanks in a Free Society (N.Y.: Quadrangle, 1972) and Records, Computers, and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education, and Welfare, July, 1973, DHEW Publication No. (OS) 73-74.

1. The "contract" theory of informational privacy

In a democratic society, which seeks to assure both individual freedom and a rationally-ordered social system, the way in which personal information is treated is of special importance. The traditional advocacy of privacy rights in information has been couched largely in civil-liberties terminology--the right of an individual to determine, in most circumstances, what information about him is obtained and used by others. But at least where organizational data systems are involved, there is growing recognition of what might be called an exchange theory. The concept here is that an individual, exercising his right to give or withhold personal information, releases valuable personal data either in order to obtain a specific benefit for himself (or his family or group, or to promote a social good he supports) or else to fulfill a legal duty (carrying the sanction of majority will under democratic theory). In return, the recipient (the data user) has two basic obligations: to use the personal information only for the purpose agreed upon(unless authorized by additional consent or by law), and not to treat the information so carelessly or maliciously that it harms the individual from whom it was obtained.

What this exchange or contract theory of information privacy recognizes is that personal information has become increasingly valuable in our data-based civilization. Our personal characteristics, once thought of solely in civil libertarian terms as entitled to protection against unwonted surveillance or disclosure, have become the vital raw material of business, governmental, and political decision-making: age, marital status, children, income, race, education, buying habits, political preferences, religious denominations, health conditions etc. If individuals were to withhold such personal information from those who daily ask for it, business and governmental affairs would be seriously disrupted, since organizational planning, administration, and evaluation depend heavily on access to such individual data. Thus, whatever it may have been in earlier centuries, personal information has become, like clean air and water, a scarce commodity today, capable of being valued in an economic sense alongside its social worth in terms of protecting individual dignity and democratic values.

Making informational privacy a property right as well as a human right does something useful in a capitalist society: it buttresses the individual's claim to assert(or at least to share) control over the uses made of his or her valuable property. It also explains why there should be a reciprocal duty on the part of the data user to live up to his side of the informational contract - not to be guilty of unjust enrichment at another's expense. Whether as a basis for legislation or judicial decision, or to explain to the public the implied-contract relationship that should be seen arising between data subject and data user, this concept has great merit for public policy.*

---

*This formulation parallels the concept of "mutuality" used in the fair information practices literature. For a recent discussion of this concept, see John P. Fanning, David B.H. Martin, and Susan Bennett, "Fair Information Practice for Health and Medical Records," a paper prepared for the Conference on the Confidentiality of Health Records, Key Biscayne, Florida, Nov. 6-9, 1974.

2. The special dangers of automated data systems

After two decades of experience with automated data systems, we should recognize that these are mechanisms highly subject to surprise.* Anyone who has followed the rapidly changing technology of computers and communication systems knows that these enormously powerful tools have--in the hands of human users--consistently done either unexpected things or expected things in unexpected ways. Each generation of computers has these "bugs" worked out, but each new generation of computer-communications technology also brings new operating principles and new constellations of hardware and software that create new "bugs" to be resolved. This is not to say that computers should not be used, or that harm must be taken as inevitable. But until we are much farther down the road to a stable and disciplined technology than we now are, we must constantly take it for granted that automated systems have a propensity to go awry. Where risks to citizen rights are involved, this calls for special attention in the planning process, and close monitoring on a continuing basis.

3. The emergence of the "data keeper" concept

For practical as well as legal reasons, it has become clear that the organization that owns a data system is the party responsible for its ethical use. Others may share that responsibility (someone else who funds the venture, regulatory-agencies, etc.), as well as those helping process the data for the owner (e.g., a computer service bureau). But a non-transferrable set of duties attaches to what the Swedish Data Protection Law calls the "keeper". These duties run in two directions--to the individuals about whom the data relate and also to the larger society. The latter duty arises because the operations of major data systems affect more than the data subjects; their operations affect the general public which hears about them, and will also contribute to general norms of organizational responsibility (or irresponsibility) in the larger society.

4. A legal duty to take reasonable care

We have already mentioned the ethical duties of data system keepers. What seems to be evolving gradually in the privacy-and-databanks debate is a general standard by which to measure the performance of those ethical duties, and to transform these into legal obligation. Simply put, this says that any organization which creates a data system that does not provide adequate policies to safeguard citizen rights and does not utilize appropriate data-security measures, creates unreasonable risks to society's interest in protecting individual rights, and should be held legally accountable for its failure to take such measures.

This notion reflects the classic "reasonable man" standard used by Anglo-American courts to measure liability in tort law. It rests on the assumption that the creation of automated information systems is generally a valuable activity for society but that it also generates foreseeable risks of harm to personal and property rights. To deter such risks of harm, there could be statutes or regulatory-agency rules spelling out what constitutes adequate policies and appropriate data-security measures for a given type of record-keeping activity or field. But even in the absence of such legislation, the standard might be applied by courts under the common law, to hold organizations liable for damages or subject to injunctive order if they had not followed the standard of care considered by the courts to be reasonable for their industry or governmental function.

---

*For a good presentation of this view, see J.J. Hellman, Privacy and Information Systems: An Argument and an Implementation, Rand Corporation Paper, p-4298, May, 1970, p. 62.

5. General requirements for demonstrating "reasonable care"

It is clear that the proper balance between claims of citizen rights and organizational needs for personal information will vary from area to area. But in every field, we are beginning to recognize that certain general standards should be observed:

A. Only information relevant to the organization's legitimate purposes should be collected and stored, and the definition of relevance must respect both constitutional guarantees of privacy and prohibitions against making improper racial, sexual, cultural, and similar discriminatory decisions.

B. The managers of a data system must take adequate steps to insure that the records it keeps are accurate, timely, and complete, as measured by the kinds of uses made of the data and the social impact of their use.

C. Detailed rules of confidentiality should govern who within the organization maintaining the data system has access to a record, and this should be based on a need-to-know principle.

D. Disclosure of personal data outside the organization that collected it should be made only with the informed and voluntary consent of the individual, obtained at the time of collection or by subsequent query, or under a constitutionally-valid legal order.

E. An individual should have a right to see his or her record, and have an effective procedure for contesting the accuracy, timeliness, and pertinency of the information in it. There may be some exceptions to this right of inspection, in the interests of protecting confidential sources, but these should be rare, and never allowed if the record is used to make judgments affecting the individual's rights and benefits.

6. The requirement of public notice

The concept from the HEW report that secret data systems should not be used to make judgments about people has been widely accepted. But beyond announcing the existence of all personal data systems lies the need for society to have the creation and expansion of data systems reported to the public in ways that indicate their potential impact on citizen rights, and that provide the basis for informed public discussion of such impact. This would be the equivalent of the "environmental impact" statement developed recently by federal and state law. The review of such notice might be lodged under a variety of supervisory authorities depending on the field involved, and there would have to be different standards for different information systems. What is critical, however, is to establish the principle that creation of personal data systems is too important to treat as an internal management prerogative.

7. The concept of independent review

Finally, the operations of every personal data system ought to be subject to regular inspection and evaluation by some kind of outside, independent body, such as a professional licensing association, regulatory agency, or governmental commission. In many cases, that independent body should be empowered to hear individual complaints about the operations of the data system, and to exercise an ombudsman function where such complaints have validity.

The concepts just discussed represent a theoretical framework for insuring that the operations of data systems are consistent with citizen rights in a democratic society. For our purposes, the challenge is to apply their general ideas to the special conditions of health care, and to the lengthening uses of health data throughout American society. It is to that task that we turn now.

B. APPLYING THESE CONCEPTS TO HEALTH DATA SYSTEMS: 12 BASIC PRINCIPLES FOR HEALTH DATA SYSTEMS

At present, there is an uneven fit between these concepts for the proper conduct of data systems and the way that American law and social practice deal with health data. Historically, the duty of physicians to keep patient data confidential, as it arose in the Hippocratic tradition, was a valuable recognition of the need for frank communication by the patient to the physician and observance of confidentiality vis a vis the outside world. But the Hippocratic tradition also embodies the ideas that physicians must protect the mysteries of the medical profession from common view, as well as to inform the patient only of what the physician feels the patient should know about his/her medical condition. These elements of secrecy and unilateral decision-making are not consistent with either citizen rights concerns or the growing "partnership" theory of doctor-patient relationships advocated by health-consumer movements. Furthermore, current law and practice as to circulation of patient data beyond the primary-care facility (through releases and implied-consent doctrines) leave much to be desired, as do the weak statements as to "confidentiality" that appear in most statutes purporting to protect health data when this is collected for social uses.

What then should be the principles that are applied to the use of medical records and health data? We will present here 12 major principles that we think need to be defined and applied whenever an automated data system is used in the health system. While we focus on automated systems, since that represents the special interest of our study, most of the principles that we discuss would apply also to manual systems, and should be helpful to those involved in those operations as well.

Wherever possible, we will illustrate policy alternatives with examples of organizations that we found presently following such innovative or exemplary approaches. In this way, we hope to show that recommended steps are not utopian proposals but policies that can be successfully and practically instituted by organizational managers.

1. Requiring Public Notice and Impact Statements

Principle

Whenever an automated data system with identified personal records is to be created for health care, service-payment, quality-assurance, medical research, or supervisory administration over health care, a notice should be filed with an appropriate outside authority and communicated to any continuing population of individuals whose records will be affected. A procedure should be provided for interested persons and groups to appear and make their views known on the proposed data system, especially as to the adequacy of its measures to protect citizen rights. To help focus that public discussion, the organization's notice should include a "privacy impact" statement describing the ways in which the proposed automated data system would affect existing policies and procedures relating to citizen rights in that organization's use of personal data.

Discussion

The notice concept proposed here is similar to that now required of federal agencies under the Federal Privacy Act of 1974. It rests on the belief that the creation of an automated data system is of sufficient importance to the individuals affected, to public confidence in the health-care system, and to democratic society as a whole that it ought not to be carried out through internal, managerial decision-making, like ordering a new photocopier or changing the paint color in the hallways.

The content of the notice would vary somewhat,depending on the type of organization involved. However, its basic elements ought to include: the data system's purposes; the types of information to be collected and stored; the regular uses intended to be made of the data; the rules for confidentiality and data-access within the organization; the rules for releasing identified data to outsiders; the provisions for access to and review of their records by the data subjects; the provisions for assuring accuracy and timeliness of data, and purging stale data; and the data security measures to be followed.

A notice system of this kind (published in the Federal Register) is already mandated by the Federal Privacy Act for federal agencies, including those involved in health activities. However, no privacy impact statement or advance notice to data populations are required in that legislation nor is there any federal commission or regulatory agency empowered to approve or disapprove a data system plan. Notice requirements similar to the federal act are used in the five states that have passed fair information practices acts for state and local governmental agencies. How well such notice systems are working so far, and whether centralized review ought to be instituted are issues we will discuss later in this chapter.

How private health organizations and all state health facilities could be brought into a notice and impact-statement system raises some difficult policy issues, especially as to the body that would receive the notices and the kind of hearings process that would be conducted. The alternatives range from the most voluntary options to the most regulated ones.

At the voluntary end of policy spectrum would be a system that required organizations simply to issue the notice, publish it in a reasonably accessible place, receive whatever reactions might be forthcoming during a waiting period, and then adopt whatever the managers considered to be useful suggestions in the implementation of the system plan.

A more supervised approach would be for some private body (such as a commission comparable to the Joint Commission on Hospital Accreditation), or a state health agency, or state fair information practices commission, or the federal Department of HEW, or a federal privacy commission, to be designated by legislation to receive such system notices and hold formal hearings on them. This plan would not lodge decision-making power in the central body but would see it simply as a collector of notices and forum for responses, possibly with a recommendatory role.

Finally, the notices could be handled in the manner of the Swedish Data Protection Board, which licenses all automated data systems, governmental or private. Under Swedish law, every hospital, health center, health insurance board, disease registry, or medical research project must furnish the kind of notice described above as part of the registration process, and the Data Board must approve the policies and safeguards before a license will be issued. Any one of the three authorities already noted -- a private body, a state agency, or a federal agency -- could be given such registration-type authority for health data systems in the United States.

There are pros and cons in each of these alternatives. A national authority that had approval or disapproval power in the Swedish style would represent a large extension of federal supervisory authority over the operations of private and state health facilities, with risks not only of over-rigid federal controls but also of potential misuse of power by federal authorities. How such a commission staffed by the President's men would have helped in Richard Nixon's quest for derogatory data on his "enemies" must be in the minds of anyone considering the creation of a federal board having control over the future medical record systems of the nation. Even if such a federal body were given only the authority to receive organizational notices and conduct hearings, or issue advisory recommendations, this would give the federal agency a considerable leverage over state and private health organizations.

On the other hand, while looking to state-government authorities to regulate themselves and private organizations would have the value of keeping supervision closer to the local level, and decentralizing supervisory power, it would probably involve a lengthy period while the 50 states enacted such measures, as well as the likelihood of inconsistencies in standards from state to state.

Going the private-commission route for private health organizations has the advantage of strengthening private autonomy and fostering self-regulation, and would probably be supported strongly by the private sector if it felt that government control would otherwise be enacted. However, the ability of a voluntary organization to enforce standards is often quite limited, and many critics of the Joint Commission would say that its record demonstrates just that point in the hospital field.

It may well be that most individuals will make a policy choice here based on their general philosophy about governmental power and private autonomy, as well as their preferences between federal and state roles in the political system. Some observers may wish to reserve judgment temporarily until some experience has been recorded as to how federal agencies have fared with the public notice requirement of the federal privacy act, to see whether more state legislation begins to fill the current regulatory vacuum, and whether private health organizations adopt such public notice techniques as a matter of voluntary practice. For the purposes of this report, the principle of public notices and impact statements has been presented as something that ought to be done, whatever the particular authority that may be installed to administer the process.

Another element of the notice system proposed here is that any continuing population of individuals that will be affected by computerization should receive clearly-written description of what is proposed *before* the data system is installed. This would include families registered at a community health center such as Martin Luther King Jr., subscribers to health insurance policies, persons working for an industrial corporation automating its employee health data, and similar groups. This concept assumes that individuals have a right to advance notification, not merely a statement of what has been done. Any person who might feel so disturbed at how this data system was being set up would then be able to assert his or her complaints, raise issues publicly, and, as an ultimate step, withdraw from being a patient, policyholder, employee, or other participant in that organization's affairs.

This idea of advance notice may seem excessive to some observers, involving some costs in money and delays in schedules for automation. But humane health care involves unique concerns about the trust and confidence of patient populations in those who are providing them with care, or paying for health services. As we look ahead to the increasing use of automated health care records, lifetime patient histories, disease surveillance registers, and other potentially valuable uses of information technology, assuring that patients feel they have meaningful control over what is done with their information, including a right to opt out of one type of record-keeping system and to choose another that better suits their values, represents an important step in democratizing the uses of technology.

2. Setting Proper Limits on the Collection and Recording of Personal Health Data

Principle

An organization creating a health data system should examine whether the collection and/or recording of each element of personal health information is essential for carrying out the organization's proper functions. Socially-acceptable standards of *relevance* and *propriety* should be worked out for the data systems in each of the three zones of health data use, through public discussion and appropriate policy-setting mechanisms.

Discussion

A. Primary Care: Zone 1

Where primary health care is being provided, from doctor's office to clinic and hospital, we saw that the current trend is to collect *and* record a wide range of information about the patient, including personal and family history, social activities, alcohol and drug use, sexual patterns, emotional and psychological problems, and much other sensitive data. Computerization leads to more systematic recording of these data, and their availability to personnel (other than physicians) sharing in the primary-care process.

Since extensive disclosure by patient to health professional is voluntarily given, is needed for effective care, and is the area of confidential communication best protected by existing law and social norms, many thoughtful leaders in the health field, including some who are strong advocates of consumer rights and civil liberties in health care, urge that new privacy rules ought to avoid any intervention as to what is collected for primary care. Dr. Lawrence Weed, for example, argues that too little personal and social data is usually collected today in primary care, not too much. In his own facility in Vermont, where an experimental automated problem-oriented record is being used, the data-collection forms and progress notes produce an extremely detailed personal, social, and medical history for each patient, and Weed sees this as a vital part of a patient-oriented health-care process.[1] Both from principle and experience, therefore, Weed is strongly opposed to law or regulation setting relevancy limits on what is collected or recorded for direct patient care.

The acceptability of Weed's position may well turn on what other rules society is willing and able to apply to the uses and flows of such health data from primary care. That is, if patients are given the right to know what is in their primary care records, if their voluntary consent is required before information is released from those records for all uses beyond primary care, and if the law were to safeguard such data far better from compulsory disclosure for non-medical uses than it now does, then society could take a favorable view of highly-sensitive personal data being recorded in primary care data systems. But if these policies and safeguards are not installed, then the claims of primary care facilities to record such extensive, sensitive information must be evaluated in terms of their likely uses and exposures beyond the care facility.

We will be discussing how to deal with patient access, informed consent, and social uses of medical records in later sections. What needs noting here is that society simply cannot accept the health professional's plea for unbounded data collection and full recording in data systems unless there are iron-clad guarantees, enforceable at law, that the patient's rights, benefits, and opportunities in the larger society will not be harmed by production of his or her self-revelations from primary-care records. This means that all health professionals who seek the advantages of extensive data collection for primary care will have to commit themselves fully to the installation of legal protections for those data, or else risk public opposition to such systems as creating too great a danger for citizen rights.

B. Service Payment and Quality-Care Assurance

When standards of relevancy and propriety are sought in the area of service payment, we must treat the underwriting/eligibility process separately from the claims process. In underwriting of private health insurance, society has -- until recently -- allowed the profit and non-profit firms to use whatever standards they wished in selecting persons to insure. Since there was thought to be no legal "right" to health insurance, any more than a right to have a food-freezer contract or a pest-exterminator for one's home, this was treated as a commercial service offered to consumers, subject only to the anti-fraud controls of general consumer protection.

During the past decade, however, using race as an overt criterion for health insurance has been forbidden by law. Offering different policy benefits to males as opposed to females within the same occupational group or other classification have been attacked before state regulatory commissions and in the courts, and the health insurance industry has recently adopted a policy against such discrimination.

The same is true of homosexuality, where regulatory hearings in Pennsylvania prompted a health industry statement that homosexuality per se would not be used as a basis for turning down an applicant. Certain physical handicaps that once were used to decline policy applications have been receiving similar reconsideration, as a result of group pressures; for example, Florida recently enacted a statute forbidding underwriters to refuse health policies to paraplegics solely because of that disability.[2]

On the other hand, health insurers do look at "life styles," and will reject persons whose health habits or style of living create special risks of health problems. These have generally been accepted by regulatory authorities, as with writing special, low-cost policies for persons who do not smoke or drink alcoholic beverages, or use addictive drugs.

Society clearly has a right to define the criteria it will allow insurers to use in writing insurance policies, in health or any other insurance line. We should recognize that what we are doing by such interventions is socializing certain risks. Since the companies cannot survive by losing money, all policy-holders will have to pay the cost of not allowing the companies to exclude persons whose conditions may, in fact, lead to higher than average costs of morbidity or disability, or earlier mortality. That is one way society can prevent continued harm being done to persons whose "objective" situation is the product of past social and legal discrimination. Whether through industry self-regulation, the state insurance regulation process, amendments to the Fair Credit Reporting Act, or recommendations for Congressional action by the Privacy Protection Study Commission, new standards of relevance and propriety in the health underwriting process should be a major effort.

Effectively monitoring these standards for compliance will involve scrutinizing the application forms of health insurers, the investigative or "inspection" reports about applicants done by their own underwriting departments or outside commercial reporting agencies, the reports of examining physicians where these are used, the examinations that are done of the individual's medical records under release procedures, and the propriety of the uses made of data properly collected. An example of the latter problem is that street address is a perfectly legitimate informational item to collect, and necessary for communication with the applicant; but if it is used to reject applicants from sections of communities known to be predominantly black or Puerto Rican, that would be a racially-discriminatory policy to be prevented.

When we turn to the claims process, we must start with the recognition that identification of the individual, description of the service provided, a diagnosis of the condition, and similar key information is absolutely essential to determine coverage (or eligibility) under a contract or program. Such data are also needed to control fraudulent practices by practitioners and institutions, and to supply a data base from which to determine future rates, coverages, and programs. As long as payment for American health care is based on a combination of the patient's funds, insurance coverages, and government reimbursement programs, the claims review process must obtain such personally-identified information. In this sense, service payers are right in asserting that they are central (and legitimate) participants in the American health-service process, not interlopers.

However, the legitimacy of the payer function has been used, too often, as an excuse for collecting and retaining more personal information for the claims process than the function requires. We found that a lack of trust in the confidentiality rules and practices of claims payers (as a whole) was widespread among psychiatrists, internal-medicine practitioners, medical record administrators and other professional groups, and was being increasingly voiced by consumer and civil liberties groups.[3]

The problems to be overcome are not, in fairness, exclusively those of the service payers. When hospital personnel find it easier and cheaper to send out a photocopy of an entire medical record or hospital discharge summary, rather than extract the specific information asked for by the payer, then the harm to confidentiality arises from the hospital's conduct, not the service payer's. Or, when some psychiatrists use vague and uncommunicative terminology in a deliberate effort to get reimbursements for patients whose condition -- if accurately described -- would not be covered by a contract or program, and this prompts the service payer to ask for more details on which to base an accurate judgment, this leads to a weakening of confidentiality for which those psychiatric practitioners must share responsibility.

The need to clarify relevancy standards for claims review has prompted a number of recent actions. For example, we noted in Part One that the National Association of Blue Shield Plans had adopted in September of 1975 a set of "Guidelines on Preserving Confidentiality of Medical Records."[4] In the section on "Internal Access and Handling of Medical Information," the Guidelines state:

> "3. Plan employees should seek only those data necessary to adjudicate a claim, case or utilization patterns and profiles."

The discussion of this says: "For example, if the Plan needs only a discharge summary or consultation report, it should not ask the hospital or physician for the entire record. To do so, not only creates storage problems, but also places unnecessary burdens on those mechanisms which are meant to insure confidentiality."

Paralleling this guideline, leaders in the medical records profession have called on hospitals "to maintain stricter quality controls on information sent to insurance companies."[5] Their proposals include hospitals requiring insurance companies to specify "why and what information is necessary" when they request data beyond that clearly necessary to review a claim, and to return to the hospital the copy of a patient's medical record within a specified period of time, or destroy it after the claims review process is completed.

Some medical organizations have been negotiating with health insurers and their associations to work out better standards. For example, the Union of American Physicians and Aetna Life and Casualty Company agreed recently on new procedures to govern payment of health insurance claims for persons covered at work by group plans. Aetna agreed to drop the questions from its claims form asking about factors responsible for the illness, the type of impairment in the patient's family, and interpersonal relations. Only the medical director of the employer-company would be given the official diagnosis and prognosis of the patient by the insurance firm. All these records would be destroyed after one year. Diagnosis of patients who were not violent and dangerous to others would not be made known to the employer or to the union; they would only know that the patient was being reimbursed for medical treatment.[6]

Model legislation is now under discussion, drafted by the American Hospital Association and the American Medical Association, that would affect the release of information by primary care providers to third parties. This would obviously affect what service payers could lawfully collect, and we will take these proposals up later in this chapter, when we consider model legislation as a whole.

When we turn to quality care reviews, the collection of detailed information about diagnosis, condition, treatment, outcome, and the like is clearly relevant, and recording such information for the care review process has become an important pressure for more systematic data collection in primary care facilities and service payer organizations. The key issue here in terms of the principle of limited data collection is whether personal identifiers can be removed from the records reviewed in this process. If this can be done, it would reduce substantially the threats that sensitive medical data about celebrities might leak out of the care-review organizations, or that information about political opponents, dissidents, and surveillance targets might be obtained by high government officials through the cooperation of government care-review emloyees or by penetration of the record system by stealth. Whether this can be done will be a particularly critical issue in securing public support for any proposed national health insurance plan, where the problem of a federal medical record system on most citizens raises special, post-Watergate sensitivities.

There are several available mechanisms to strip names and other unique identifiers from each record and substitute a special review number. This can be done by the facility holding the original record, as with hospitals in the PAS system described in Part One. If it is necessary in certain cases to bring together records on the same individual from several facilities or different organizations, a special agency, private or governmental, could be given the job of combining the records and forwarding the needed information with only a review code number as the identifier. If attention is paid to removing from the record other revealing information not really needed for care review -- such as the occupation of a person as entertainer or federal executive employee -- there should be few reasonable fears about identities breaking through records even though names are not on them. Should situations arise in which contact with the patient is necessary to resolve disputed facts or issues, those would be handled as exceptional cases, and this ought not to be cited as justification for having identifiers on each record reviewed.

Given these practical procedures, we suggest that the burden of proof should be on each quality-care review system to prove that it cannot operate under a system without unique identifiers; absent such a showing, it should be the duty of care review organizations to devise a system that does not use or store identified personal records.

C. Social uses of medical and health data

When society should require the production of health data for non-medical uses has come under serious re-examination in the past decade. We saw that this was sometimes a matter of rethinking the relevance of physical handicaps or emotional and mental status for decisions about employment, licensing, public housing, etc. Sometimes the issue was how relevant past health conditions might be for making present decisions about people, especially where there had been a change in society's attitude toward a once-stigmatized condition (e.g., abortion). Still another issue has been how to deal with recording the health data of minors, with special problems of minor-parental relations and leakage from juvenile care into the larger society.

The employment area is a good one to illustrate the application of the relevancy principle. We noted earlier in this report that lawsuits are now pending which challenge the right of government and private employers to ask for general information about emotional and psychological conditions on employment applications. Opposition to "intrusive medical questions by employers" has been registered by the Privacy Committee of the American Civil Liberties Union, which has prepared a policy statement opposing such practices for adoption by the ACLU National Board of Directors.[7]

Apart from government licensing requirements that include health tests (airline pilots, persons working in food establishments, etc.), most employers give job applicants health questionnaires to fill out. Some employers also require the completion of a health report by a physician, either the patient's own or one supplied by the employer. The typical health forms ask not only about standard diseases and health conditions but also histories of past conditions (e.g., bedwetting) and about past and present emotional problems, nervous disorders, and related psychological matters, including whether the individual is presently receiving psychological help.

Employers justify these inquiries in terms of securing employees who will be able to perform satisfactorily on the job, will be likely to remain long enough to justify the heavy expenditures for training and promoting employees, and to keep the employer's group health premiums (which are based on utilization patterns) as low as possible. In a free labor market, most employers would assert, selecting healthy employees from the pools of job applicants is a legitimate exercise of employer choice, comparable to selecting the best educated, most experienced, and best performers on aptitude tests.

As with many areas once under complete employer prerogative, American society has imposed substantial limitations on employer selection policies during the past decade, in both governmental and private employment. If educational requirements or tests prove to have the effect of screening out minority racial applicants, for example, or reducing minority employment opportunities, the burden is placed on the employer to show that the educational requirements or tests are relevant to the jobs involved, and that they do not incorporate racial biases. Similarly, even physical requirements for jobs (such as height requirements) cannot be used against minorities or women unless they can be shown to be essential to the performance of the employment, a standard that the courts have used recently to strike down many such physical conditions. In addition, federal legislation in 1973 on the employment of physically and mentally handicapped persons recognizes an obligation by employers to provide special physical facilities that may be needed so that handicapped persons can carry out jobs, thereby wiping out the excuse that many employers traditionally used to explain why they could not hire persons in wheelchairs, using crutches, etc.

In part, calls to reconsider health standards for employment have come from practitioners of occupational medicine, who regard many current practices of corporations as unwise. A study by two Veterans Administration doctors documented that industrial physicians would recommend against hiring persons with conditions such as angina, previous myocardial infarction, diabetes, hypertension, and previous psychiatric illness, with the reasons cited including fear of company liability for further illness and increased insurance costs. The doctors concluded that such restrictive policies are denying work to "patients with mild illnesses, which may not increase their morbidity or mortality," and that the criteria used "have little relation to modern medical judgment." Furthermore, the authors voiced the concern that "with automation of hospital records, retrieval of medical data will become easier, and it may be impossible for an applicant to conceal a past or present illness, however unimportant." This increase in record-keeping trails coincides with a trend toward discovering diseases "earlier in their course with the use of newer diagnostic techniques," making the problem of employment for patients who have various mild illnesses "even more widespread."[8]

Some companies have altered their pre-employment health questionnaires to take account of citizen rights concerns. The IBM corporation, for example, used to require applicants for employment to answer a question about receiving prior treatment for a nervous disorder, mental problem, or emotional difficulty. A privacy review within IBM during 1974-75 showed that this put applicants in the difficult position of answering truthfully (and risking a turn-down) or lying about receiving professional help for emotional problems (and starting their employment relationship with the company on a resentful and dishonest note). The IBM review also disclosed that many psychiatrists were counseling their patients to answer "no" to such pre-employment queries when the patient's condition did not indicate any inability to carry out the employment; that many middle class parents were fearful that arranging therapy for their children could lead to curtailment of their future employment opportunities; and that there was no medical or social evidence that persons who were receiving professional help for emotional problems were worse employment risks than persons of similar educational and social backgrounds who were not receiving such help. After weighing these problems against the assumed benefits to be gained by forcing self-declarations from applicants, IBM dropped the question from its pre-employment questionnaire in 1975.[9]

Developing new standards for collecting health data in the hiring process is an example of a priority area for action in Zone 3 activity. The ACLU Privacy Committee suggests that "the employer's legitimate interest in an employee's health extends only to the employee's present ability satisfactorily to perform the job sought," and "this interest must be satisfied by the least intrusive means available."[10] An employer who wishes to verify that ability should pay for a medical examination, with the employer "entitled only to the physician's certification of the applicant's ability or inability properly to perform the job as described to the applicant and the examining physician." Whether done by the applicant's own physician or a company physician, all medical information obtained by such an examination "shall be privileged and confidential" and not revealed to the employer.

This recommended policy is one that also coincides with IBM company practice. While less than 2% of IBM applicants are not hired for medical reasons, Dr. John Duffy, IBM's medical director, notes that 5% of its employees fall within U.S. Bureau of Labor standards of handicapped workers, and approximately 20% of IBM employees are subject to medical restrictions (e.g., controlled diabetic). When applicants are given pre-employment physicals by IBM physicians or outside consultants, the results are kept confidential, and IBM managers are not told the specific health reasons if work restrictions are set by the company medical department for new or existing employees. An employee's health condition is never included in IBM's personnel data system.[11]

Our discussion of collecting health data on job applicants illustrates (as we have noted before in this report) that the relevancy and propriety issues for data systems usually raise deeper questions of social policy. There is no necessity that the questions be raised in the context of records and data systems, rather than more directly. But the reality is that this is often the way that affected groups and public-interest organizations can bring the problem to public attention. Since the building of new data systems brings these policies up for organizational examination in terms of data collection costs and efficiencies, this is the ideal opportunity for society to insure that proper citizen rights policies are instituted.

3. Notifying Individuals of Data Policies When Their Information Is Sought

Principle

When an individual is asked to supply personal information to be included in a health data system, he or she should be given a clearly-written account of how that information will be used by the collecting organization, and what procedures for obtaining consent will be followed before any additional uses will be made within the collecting organization or identified information is supplied to other parties.

Discussion

Following the contract or mutuality principle, the Federal Privacy Act and its state counterparts require that individuals be informed, at the time that their information is sought, of how their data will be used and what the organization's rules for data sharing are. Simple and equitable as this sounds, it has not been the practice among many health organizations, generally on the assumptions that people don't really care and that it would only stir up unnecessary anxieties. Though experience to date needs to be systematically canvassed by the Privacy Commission and other bodies, the impression drawn by our project from contacts with various federal health agencies is that such notification has been going fairly well. Agencies have included notices on their data collection forms, have displayed posters in their offices, and have obtained signed acknowledgments from the individuals indicating that they have been informed of the policies and give their information after being so informed.

The one complaint that we have heard involves fears that an organization might want to use personal information for an important purpose later that would not have been described and assented to at the time of original collection. An example cited to us was that data relating to the effects on patients of using a particular drug many years earlier might not be available for follow-up research, as when there is some reason to believe that a birth-control drug used ten or twenty years earlier might now be producing cancer in those who took it. To ask the patients for consent to use their later data in the hands of the hospital might alarm them unnecessarily, before the possible effects have been confirmed.

Rather than abandon the principle of describing present and future uses at the time of collection, we think that explanations developed by various kinds of health facilities and organizations should be drawn up with such possible contingencies in mind. It does not seem beyond the ingenuity of experts in medicine, law, and administration to encompass these in a notice. If some unforeseen development occurs later, either subsequent consent could be obtained or the additional use might be authorized by an independent review body set up to supervise health data systems in a particular field and insure protection of citizen rights. Whatever technique may be developed, the basic point is that citation of hypothetical future possibilities should not be allowed to overcome the requirement of notice.

4. Information Release Forms Should Be For Specific and Limited Purposes

Principle

Because the trend in automated health data systems is to record and retain personal information more fully and systematically, general release forms do not meet proper standards of citizen rights. The forms used to release personal information from a health data system should be for a specific purpose, should describe the information to be released, and should be limited in the time period for which the release applies. Adequate procedures must be followed to obtain the individual's voluntary and informed consent to any release. Provision of entire medical records under release procedures should be permitted only upon use of a special release form, reviewed by a special officer of the record-keeping organization. Organizations seeking release of information must file with the record custodian a form indicating how they would use the data, specifying that it will not be released to other parties without the individual's consent, and indicating what the retention or destruction policies are for the information so obtained.

Discussion

The general release in the health field brings to mind the general warrants to search and seize used by British officials in our colonial era, against which the Founding Fathers fought so bitterly and which they forbade by the Fourth Amendment to the U.S. Constitution. Among the vices of the general warrant were that it authorized anyone holding it to engage in a search; did not indicate the purpose and thereby define the proper scope of the search; and did not specifically describe the things to be searched for and seized if found. While the law enforcement and health-care settings are very different, the analogies in civil liberties theory are, alas, all too close.

Individuals are being asked today to sign releases that allow the custodian of the individual's medical record to disseminate its contents however, and to whomever, the custodian feels necessary, or that allow someone who is offering a benefit or service to the individual to examine "any and all" medical records in any doctor's office or health institution to which the inquiring party shows up, armed with the general release. The absence of informed consent in such situations is proved by the fact that individuals in most health institutions do not know (and are not told) what personal, family, social, and medical information is in the records that will be opened for inspection. Even if they do know generally what is in their records, they are not told which segments of this the insurer, licensing body, employer, welfare department, etc. will have access to. They are also not told what will happen to their information after the party to whom it is released has made its decision (whether it will be destroyed, passed on to industry data pools, stored permanently by the third party, etc.).

Such practices, bad as they were in the manual-records era, cannot be permitted to persist in the era of large-scale health data systems, with increasingly comprehensive records being generated and preserved in primary health care facilities and in special medical files. One can understand the motivations of the health providers in seeking the broadest possible release to avoid legal liability for releasing information without permission, and by the third-party inquirers in seeking access to anything that might prove to be relevant when they go to make their determination in a specific inquiry. But allowing such motivations to justify the use of general, all-purpose releases is to allow the inferior bargaining position, fears, and temporary dependency of persons receiving health care to be legally institutionalized, just as the law used to accept similar disadvantages for consumers, debtors, and other groups in unequal bargaining status to large institutions. Just as the latter abuses have recently been overturned by legislation and court rulings, we ought to overturn abuse of power in the handling of information releases.

There are health centers and hospitals which take exemplary positions in this matter. We saw in the profile how the Martin Luther King Jr. Health Center required patient consent to the release of information. Here is the recommended policy for neighborhood health centers, as presented in an excellent guidebook on confidentiality published under OEO auspices in 1971:[12]

> **Release of Information with Informed Consent**
>
> The health center should not divulge confidential patient information contained in patient records without obtaining a signed release from the patient, unless (1) there are statutes to the contrary, or (2) there is a serious emergency requiring release without consent. Does this mean that the health center *must* release patient information whenever it receives a signed patient authorization? The answer depends largely on the statutory and case law of the state. In general, consent is not considered valid unless it is *informed consent*, i.e., the patient fully understands what he is consenting to. Even in states where the law requires release when patients have signed consent forms, health institutions must take precautions to protect the patient. The medical record librarian should take the five steps described in detail below.
>
> *Require the patient's signed consent.*
>
> The patient may write his own letter of consent or sign a standard form, such as a health insurance policy form. If the patient writes his own consent statement, he should state specifically *to whom* the information is to be released and exactly *what* information is to be released, and he should *sign and date the request*. The librarian should check the patient's signature against a previously obtained signature, and note the date to be sure that the request is current. It is advisable to set a maximum length of time, such as 90 days, after which the request is no longer considered current and will not be honored. If there is reason to believe that the authorization is not genuine, or if it is not current, the medical record librarian should withhold the information until she has received a valid, current authorization from the patient. One way of determining whether the request is genuine is to contact the patient by phone.
>
> Patient consent for release of information should not extend beyond a specific illness or its subsequent treatment. If an authorization carries a date which is prior to the date of the requested information, the medical record librarian should determine if the authorization applies to the specific illness for which information was requested. If the authorization pertains to a different illness or treatment, a new consent form should be obtained. Each health center should have its standard consent forms reviewed by an attorney to make certain that the forms adequately protect the patient and the institution.

> *Establish that the patient understands what information is being released and to whom it is being released.*
>
> This is important to ensure *informed consent*. It will not be feasible to check with the patient in every case, but it is important to contact the patient if there is reason to doubt that his consent is truly informed.
>
> Because of the pressure that is often exerted on people to sign printed forms, center staff members may wish to educate all patients about the consequences of signing various kinds of forms.
>
> *Send out only that information from the patient's record which is specifically requested.*
>
> For example, the health center should withhold psychiatric and social information unless it is specifically requested. If an insurance company or the State Industrial Accident Commission seeks information regarding a particular accident, the health center should withhold information recorded before the date of the accident unless the information is included within the scope of both the request and patient's consent.
>
> *Inform the patient's physician or the appropriate team member that information is being released.*
>
> If the record contains particularly sensitive data, consult with the physician before releasing any information.
>
> *Be reasonably certain that the institution or individual to whom the information is being released will keep it confidential.*
>
> It may be impossible to receive a guarantee of continued confidentiality in every case, but the health center may wish to consider requiring such a guarantee, in writing, from any institution or individual that receives a great deal of patient information and from any institution or individual whose willingness or ability to guard the confidentiality of patient information is in question.
>
> Health care providers from different agencies may legitimately communicate verbally about a patient without written consent when they are cooperating in the care of the patient. For example, when an elderly person is being cared for by a public health nurse from another agency as well as by a family health worker from a neighborhood health center, many informal communications between the providers are legitimate and necessary and do not require written consent. However, health center staff members should make certain that they have the patient's understanding and *verbal* consent, in order to avoid invading his privacy or making communications that the patient himself would not make.

While this illustrates the kind of sensitive policy that some neighborhood health centers are already using, largely for manual record systems, we think that more detailed and protective policies can and should be used in health data systems. These involve specification to the individual in written form of the organization or persons who will obtain the data, the purpose for which the information is sought, the specific data that would be supplied, what will be done with it once the stated purpose is completed, and what promises the party obtaining the data makes as to its safe and secure treatment. Such releases should only be for a limited time period (such as 30 or 60 days). The consequences to the individual that might occur if the information is supplied -- or not supplied -- should be clearly explained, so that he or she could decide whether to reveal or withhold the information. (The Georgia mental health center study we discussed earlier in this report indicated that many persons receiving medical services would not consent to disclosure of their records to state health authorities if they could be assured that this would not jeopardize their continuing to receive medical assistance.) Release forms should be revocable by the individual within a specified time, and this right should be fully explained, including, of course, the potentially harmful consequences to the individual of such revocation.

One interesting proposal made by Dr. Simon Auster, a Virginia psychiatrist and expert on citizen rights issues in health care, is to give the patient in any health care setting an advance copy of the information that is to be released. The statutory language he proposed would be as follows:[13]

> "No information identifiable to the patient shall be released by the hospital, facility, agency or physician without the patient's express permission, except (1) as may be ordered by a Court of Record, in which case, the patient must be given prior notice of such order and may contest it in the customary manner, or (2) where the patient has a communicable disease, the reporting of which is required by law, in which case the patient must be informed that the report is being made."

* * *

> "The patient may request, and will be provided with copies of any other information the hospital, facility, agency or physician proposes to release to any other parties authorized by the patient to receive it. The patient may rescind his authorization to release the information within two weeks after receiving his copy. No hospital, facility, agency or physician shall release any information about a patient on the basis of a blanket authorization without first obtaining specific authorization from the patient. At the time the patient is requested to authorize the release of information, he shall be informed of his right to receive a copy of the information in advance, and of his right to rescind the authorization within the prescribed period if he wishes."

An important aspect of Dr. Auster's proposal is that it brings the element of patient notification to bear even when statutory law may require the reporting of communicable disease (and the patient cannot prevent the reporting). In fact, as we saw in Part One, current statutes require the reporting of many more conditions than communicable disease, such as gunshot wounds or child-abuse injuries. Presumably, legislatures considering new medical confidentiality codes would decide which existing reporting duties should be retained, and could apply the patient notification principle to those areas as well.

5. Increasing Patient Access Rights to Their Own Medical Information

Principle

Individuals should have a general right to information about their health condition, treatment, and prognosis, as a matter of fulfilling the professional's fiduciary duty and protecting the patient's ultimate primacy in choosing his/her own health destiny. In health data systems, an individual should have an absolute right to inspect any recorded data about him or her that is used to make judgments about eligibility for health programs and coverages, claims payment, or other aspects of service administration. The same absolute right of access should be provided when health data are disseminated to determine rights, benefits, or opportunities outside primary care settings, as in insurance, employment, licensing, education, welfare, etc. A procedure should be provided for explaining medical terminology where this is necessary, and for allowing the individual to challenge the accuracy or completeness of the recorded data.

Where that part of the medical record is involved in which the health professional's working notes or other speculative, informal recordings are present, or where they are sensitive judgments about the patient's emotional condition that might unduly upset the patient to see, and these materials are used solely within the primary-care facility, a procedure should be afforded that gives the physician an opportunity to explain to the patient why access would not be desirable, or to suggest disclosure to another physician of the patient's choice; but if the patient is not persuaded by these counsels, a right of access should be provided to patients in either chronic and acute care. Where psychiatric care is involved, disclosure of the record directly to the patient over the advice of the psychiatrist would require an order from a civil court.

Discussion

Whether an individual should have a right of access to his/her medical record in a health data system raises the most complex and controversial issue of this study. We found thoughtful and ethical positions on both main sides of the debate, and there are vexing complications in all the reform proposals that have been advocated. For these reasons, our discussion of access will be more extensive than with any other principle presented, and we will first summarize the existing state of policy conflict and law to have this at hand for our analysis.

Underlying the basic access debate are two competing models of how information should be controlled in the doctor-patient relationship. The traditional model, still dominant in the medical profession and among health administrators, is the "doctor's judgment" approach. It assumes that the expert, ethically-bound physician ought to decide what information is made available to the patient, based on the professional's judgment of what will be in the patient's best interest. This model rejects any notion of a patient's right to "full" information for several reasons: complete disclosure might create needless anxiety or upset a patient unduly; telling only part of the truth, or withholding information temporarily, may be good medicine in a particular situation, especially where psychosomatic aspects are involved; patients would not be helped if they were to be told the speculative and tentative hypotheses that physicians were considering at a given moment; and, especially in psychiatry, the patient may be so emotionally incapable of handling truthful information that its disclosure would be positively harmful. A good doctor, it is said, should disclose every bit of information that will advance good care, but this must ultimately be the doctor's decision, and one not subject to delegation to any other authority.

The more recent model of information control rests on a "consumer" theory of health care. It sees the physician as an agent of the patient, hired to exercise his/her professional skills and judgment but also bound by a fiduciary duty to make full disclosure to the patient if and when this is demanded. Such a right to full information is seen as important for the following reasons: it is essential to the patient in making informed decisions about the risks and benefits of proposed treatments and operations; it is essential if the patient is to know whether to authorize release of his/her medical information to third parties; it fosters patient participation in and taking responsibility for his/her own health care; it would assist patients in making consumer judgments about the acceptability of care being provided by a given doctor or hospital, compared to other available alternatives; and that while some patients may be so emotionally distraught that they cannot handle full information, those adult patients who ask for full disclosure of their condition and prospects should not be denied it, including those situations of terminal illness where a particular patient wants to be able to decide how to use the remaining period of life.

At present, American case law does not clearly resolve the conflict between these two theories, and each can point to some decisions advancing its position. In support of the consumer notion, the courts have held that a doctor must inform the patient of all the risks and potential outcomes of any dangerous procedure, and to withhold anything that might be relevant to the patient's decision constitutes a failure of duty. On the other hand, in ordinary care, the courts have upheld the doctor's right to decide what information to disclose to the patient and his family, as a matter of professional judgment of the patient's best interests.

When the disclosure issue shifts to the question of access to medical *records*, several additional arguments are added to the basic positions held by each model. In behalf of the consumer position, it is argued that: medical records today, especially in group practices and hospitals, are compiled by a variety of health professionals and used by various persons giving care, making it essential that a patient who feels that mistaken or erroneous data has gotten into the record should be able to see and correct it before care decisions are made in reliance on wrong data; examining what is recorded is the only way patients can decide intelligently whether to release some or all of it for service payment or social-use purposes; providing access would lessen the need of patients to file malpractice suits just to see what was in the record; and showing patients their records on a regular basis would improve patient confidence in care and enhance patient cooperation in treatment. If the records today are not written in language that would be intelligible to patients, the consumer position contends that explanations should either be added to the record or made to the patient orally by health professionals.

The doctor's judgment model, in opposing a right of access to records, responds along the following lines. Medical records are generally written in technical and jargonistic terms that communicate to fellow professionals but that patients would not understand, and having to explain these constantly to patients would be an unnecessarily time-consuming and expensive procedure; having to write notes and observations constantly in a way that would be diplomatic when read by the patient would impair the directness and clarity of present record-keeping; providing access would inhibit doctors from putting down the speculative and hypothetical comments they now do, to help both themselves and other professionals who may later consult the record, and would lead to highly defensive record-keeping practices; and all the above pressures would make medical records much less valuable in the future for service payment, medical research, care-review, and similar uses.

As with the right to information, existing law on access to records can only be called inconclusive. In the great majority of states, there is no legislative or judicially-declared right of general access by patients to their own records when these are in the doctor's office or hospital, though the law recognizes the patient's right to have the records sent to a new doctor or hospital, or to have the physician furnish record data for care payment purposes. While only a few states have enacted a general right of access statute, any patient who files a malpractice action is able to secure the entire medical record for the purposes of the litigation. Federal agencies providing health-care, such as the Indian Health Service or Veterans' Administration hospitals, are now governed by the Federal Privacy Act of 1974, which sets a general right of access by individuals to their federal records, with no exemption in the statute for medical records. However, regulations issued by federal health-care agencies have specified that, if the federal physician feels it is called for, disclosure of the patient's record can be limited to an outside physician selected by the patient, who would then decide what to disclose to the individual.

While the two basic models are usually advocated for every type of health setting, some commentators suggest that society's response might well apply different rules depending on what kind of care is involved. For example, the management of chronic illness and rehabilitative medicine in clinics and doctor's offices, with a focus on continuing-care relationships over substantial periods of time and the need for patients to cooperate actively in health regimens, has been seen as the most favorable setting for a patient right of access. On the other hand, psychiatric care has been described as the least favorable, since it is assumed that so many patients in private or institutional care are likely to be harmed by a policy of automatic disclosure. This leaves acute care--the typical hospital situation--as middle ground.

Having summarized the arguments for and against access rights, one last point of background is useful. On the whole, automation of patient histories and medical-record applications both accentuates the problem *for both sides* and offers some interesting possibilities for working out practical solutions.

Computerization accentuates because(as we noted) it leads to richer and more complete patient records. This makes *patients* more concerned about what is now captured in their records and disseminated efficiently beyond the primary care setting, and makes *doctors* more worried about having their detailed progress notes, formal diagnoses, and observations on emotional and social aspects printed out for patients to take away, and often to show to their lawyers and friends. At the same time, compared to the handling of manual or microfilmed records, the computer makes it much easier to print only selective portions of a record, under rules of authorization, and to suppress securely all parts of a record that are not to be displayed or printed to a given inquirer--patient, insurance company, researcher, policeman, etc.

Recognizing the persuasive aspects in each basic view of disclosure and good health care, policy choices still must be made. The ones we recommend move toward increasing patient rights of access. Two central considerations help us to reach this judgment. First of all, for most Americans today, health care is simply no longer the one-on-one, family-physician situation in a Dr. Kildare and Marcus Welby type of personal medicine, where the individual's personal and emotional life, job problems, and family relations are intimately known, over long periods of time, by a single physician or small group practice. For the majority of Americans, care by a succession of doctors and nurses in group practices, clinics, and hospitals is the rule. Given the mobility of Americans for schooling, occupation, and residence, changes in such physicians and institutions are frequent. And even those patients who have access to one regular, general practitioner will be treated by a series of specialists and institutions for particular problems. In this setting, it makes no sense to install a national legal rule as to patient access that is geared to a treatment situation of sustained personal relationships that covers only a small minority of the patient population.

Secondly, we are entering a period of change in the format and content of medical records, spurred not only by dissatisfaction within the medical profession that has prompted problem-oriented record reforms, but also the tremendous pressures to redesign records in order to meet increasingly strict payment and care-review requirements. This condition of change being the case--and with the information-handling capabilities of the computer to draw upon for innovative solutions--American society ought not to allow the present character of medical records to control the decision as to what would be the best access policy for the future, especially for automated health data systems.

For these reasons, we suggest that health data systems should move toward a two-tier or "dual" system of medical records. The first part, which would come to be considered the official record, would consist of all personal data about the patient; social and family history; complaints, tests, and examination results; diagnoses recorded; treatment summaries, drug regimens, etc.; payment information; and any other sets of data that were to be recorded as official. The patient would have a full right of access to this part of the record, with a procedure to explain medical terminology or the implications of diagnoses.

The second part of the record would consist of any especially sensitive judgments about a patient's emotional or psychological condition or speculative and tentative hypotheses that a health professional wanted preserved for his/her own use, or that of others sharing in direct, primary care. Such materials would not be available for any other uses beyond primary case. It would be reachable through subpoena by the patient in a malpractice case, just as such physician's notes are now. Obviously, then as now, anything a physician did not think it safe or wise to write down would not become part of any record, a prospect that would at least prevent the circulation of such data to third parties.

The idea of dual record-keeping has been endorsed recently by an interestingly varied set of commentators, such as the American Society of Internal Medicine, the American Civil Liberties Union, and the IBM Medical Department.[14] The concept rests on preserving the confidentiality of especially sensitive professional commentary within primary care while recognizing that the patient's interests in protecting his/her rights in service payment and social uses of medical data must be insured.

We recommend that different procedures for patient access to the second part of the dual record be followed for chronic and acute care on the one hand, and psychiatric care on the other hand. For chronic and acute care, those physicians or institutions that wish to do so ought to be encouraged to experiment with regularly giving patients copies of their entire problem-oriented record, as is being done with considerable benefit in several hospitals already.[15] Where this is not the policy followed voluntarily, a three step process should be required:

1. The health professional supervising the patient should have an opportunity to discuss with the patient directly why the professional feels access to the second part of the record would be medically or psychologically unwise.

2. If the patient is not persuaded, the health professional should be able to recommend that disclosure be made to another physician of the patient's choice, who could then decide what to reveal to the patient.

3. If the patient rejects both these options, the patient should have the right to see the record. Essentially this is on the theory that there has already been a collapse of trust in the doctor-patient relationship and it would not be good medicine or in the patient's best interest to continue to refuse access at that point.

Psychiatric care raises special problems, since many patients in therapy--though by no means all--may be so emotionally disturbed that they could not "handle" such information from the second part of a record as diagnostic terms, observations on their personal histories, etc. Where there is individual psychiatric care in a one-to-one relationship, non-institutionalized, we recommend the same first two steps described above but a different third step. If the patient still wishes to have access to the record after the psychiatrist attempts to dissuade him/her, the record would be provided unless the psychiatrist felt withholding it would be so important to the patient's well-being that the psychiatrist is willing to end the therapist- patient relationship. If such is the case, the record could be withheld unless the individual applied to a civil court to have the record disclosed. The court would hear in chambers the arguments of the health professional and the patient and then decide whether direct disclosure was to be ordered.

Where individuals are institutionalized, the need to protect their rights against abuse, especially in state mental facilities that may be providing inadequate care, makes a third-step court proceeding brought by the individual or his/her legal guardian the desirable procedure. This is essentially what the court did in granting parents of retarded children at Willowbrook in New York a continuing right of access to the medical records, as part of a suit brought against the institution to insure adequate care.[16]

As we suggested earlier in this discussion, the computer makes it quite feasible to store all the data about a patient in one file that has different access codes to control display and print-out of two different segments or even to store the sensitive second part of a medical record on a minicomputer apart from the main patient files. Audit trails can be established to document who uses the "internal" segment, and a general inspection and testing of the dual record system would be made periodically by the reviewing authority we have already proposed.

There is little doubt in our minds that the suggestion for a dual record system and giving patients access rights will be vigorously rejected by many medical practitioners and health administrators today. It may be that it will take years of experience with Federal Privacy Act access procedures, with further voluntary projects such as those being conducted by Dr. Lawrence Weed, Dr. Arnold Golodetz, and others; and with corporate programs such as that of IBM before a majority of the medical profession would be willing to accept these ideas with enthusiasm. Some persons such as Dr. Golodetz suggest waiting out that period, and counting on example and advocacy to persuade.[17] But this assumes that we have a good deal of lead time, an assumption that must be examined in terms of when a national health insurance plan might be enacted, major expansions of health data systems might go forward in hospitals, and major regional data systems might be developed. When such major steps are taken, we suggest that the line has been crossed at which the intervention of law ought to take place, at least for the records in those health data systems.

6. The Duty to Insure Appropriate Accuracy

Principle

The managers and staff of a health data system must take steps to see that the personal data they store are as accurate, timely, and complete as the uses to be made of them require, not only to assure the individual's proper health care but also to protect the social opportunities and benefits of individuals that may be determined through use of such data. Participation of the individual in review of his/her records before release to third parties, and affording individuals a general right of access to their records, represent helpful ways to improve accuracy in such data systems.

Discussion

Throughout our project, in studying the literature and making our site visits, we saw that errors of personal information, faulty recording of test results and diagnoses, and failure to complete necessary record items were persistent problems of record-keeping in hospitals and doctors' offices. When records are automated, their use by many members of a health team, or their circulation throughout a multi-unit facility or regional health organization, or reliance on them for producing payment, claims, and social-use data all make it important to assure the accuracy of individual records.

When an automated system is properly designed and administered, it can increase traditional accuracy levels. For example, we saw automated systems in which failure by health professionals to supply the information called for in reports would produce "tickler" notices to the professionals that such omissions had occurred, as well as notices to data processing staff or administrators to take follow-up action if the data were not furnished within a certain time. Orientation and training sessions also helped increase the commitment to supply required data. Tests for the internal consistency of data in a record can be written into software programs, thereby catching some mistakes that would have gone unnoticed in a file of paper sheets.

We also saw that accuracy was improved when patients undergoing automated multi-phasic testing in hospitals or corporate screening programs were given a printout of their personal data, histories, and previous test results, and would correct inaccuracies that they noticed. The same improvement in record accuracy and completeness took place with the use of automated problem-oriented records given to patients in Dr. Weed's center, and with the admission plan and discharge summary provided to patients in the Vermont rehabilitation center project described by Dr. Golodetz. Greater use of such patient reviews in primary care or of subscriber reviews in health insurance would certainly lead to a higher level of accuracy in records.

Whether or not patient access is afforded, managers of health data systems must take effective steps to see that records are accurate, timely, and complete. What these standards mean in a given data system will have to depend on how the records are being used. For primary care, reliance on the result of an outdated lab test instead of doing a new one before making a medical decision or going ahead with a drug dosage or operation would obviously be unacceptable. Similarly, accepting a recorded diagnosis that came from a source or a situation that was less than completely reliable (a school nurse's comment that a child's fit looked like epilepsy) would be an equally poor reliance on "the record."

The basic point is that the more comprehensive a health data system, and the more its records are relied on, the greater the attention that must be paid to accuracy, with a resulting commitment of personnel resources and systems controls.

7. The Duty to Apply Appropriate Data Security Measures

Principle

Because of the sensitivity of the personal information stored in a health data system, security measures must be taken to limit access by personnel within the organization to those with a need to see particular information items in a record, to monitor data uses in order to detect unauthorized conduct, and to protect files against outside penetration.

Discussion

Providing adequate data security represents one of the least controversial principles for health data system managers to follow: everyone will agree that it is necessary and there are well-understood techniques that computer experts know how to apply. The key issues that arise are (1) the need for management to formulate clear policies as to data access that data security measures can then carry out; (2) the need to make assessments of the foreseeable threats to data security, based on prior breaches of information security or new risks posed by especially attractive records; (3) the need to adopt a blend of security measures (locks on terminals, passwords or cards to access files, audit trails to monitor use, etc.) that will provide as much security as a reasonable expenditure of money and personnel can produce; and (4) the need to adopt special measures to safeguard files of unusual sensitivity, such as psychiatric records in a general hospital, as by storing such data on separate minicomputers in locked facilities.

Just as no data system can be 100% accurate, so no system, manual or automated, can be made 100% secure. This is true even in national defense and intelligence computer installations, where huge sums are spent on security measures and elaborate screenings and surveillance of employees are used. The basic goals of data security in health data systems should be to block or detect attempts by the organization's own personnel to obtain confidential data they are not authorized to have, and to make the cost and trouble to outsiders of breaking into the system sufficiently high as to dissuade almost everyone from trying it, or defeat them when they do. Computer manufacturers, consulting firms, industry groups, and a variety of governmental agencies can usually supply whatever assistance organizational managers and their data processing staff may need. The adequacies of security measures can be measured, in part, by the history of threats to confidentiality in that type of organization.

8. The Duty to Inculcate Respect for Citizen Rights

Principle

Since there is a great gap between publishing organizational rules or enacting legal rights and achieving positive compliance with their spirit and letter in daily life, every health data system should develop orientation programs, interpretive guidelines, continuing seminars, problem-solving sessions, special training materials, and annual reviews, to foster understanding and acceptance of the system's policies on citizen rights by the organization's own personnel. Such programs should recognize and deal with the special attitudes of major occupational groups in the organization (doctors, nurses, other health workers, administrators, data processing staffs, etc.). Wherever possible, patients and public representatives should be included in the development, management, and evaluation of these educational programs.

Discussion

Operating a health organization and its data system under the kind of ethical guidelines proposed here cannot help but disturb customary ways of thinking and behaving by organizational personnel, especially the medical professionals. Every organization that we studied which made important changes in its policies to promote citizen rights had to develop initial guidelines for its people, conduct orientation sessions, review progress and problems on a regular basis with its full staff, and compile new guidelines and procedures on the basis of experience. The promulgation of patients rights at the Martin Luther King Jr. Health Center, the IBM Corporation's revision of employee privacy policies and procedures in 1974-75, and the way Drs. Weed and Golodetz managed their patient-access-to-records projects are vivid examples of the planning, communications, and evaluation efforts that go into achieving support for innovative policies in an on-going organization.

In calling for such supportive activities, as countless studies of change in business and governmental organizations attest, the attitudes of the top management play a central role. If the central administration and department heads of any organization are only formally committed to the new policies, communicating a spirit of resentfulness and annoyance at this "intrusion" into their more important affairs, this soon communicates itself throughout the staff and sabotages positive compliance. In the examples of outstanding supportive programs mentioned above, the commitment of each organization's leaders was highly positive, and this was unmistakably communicated throughout the organization by both word and deed.

It can be noted that these were citizen rights reforms initiated by the leadership itself; securing management enthusiasm for policies that are required by new legislation, court decisions, or professional codes may be rather more difficult. For example, we found a less-than-enthusiastic attitude toward some of the Federal Privacy Act's requirements among several federal agencies in the health field that we contacted. Despite this difference between voluntary pioneers and law-compliers, it is still vital to the movement from new policy to daily observance that each organization take the kind of steps we have described.

9. The Need for a Patient's Rights Handbook and a Patient Rights Representative

Principle

Every health data system in primary care should publish a clearly written guidebook on patient's rights and responsibilities that is given to an individual at the earliest point of contact with the facility. Each system should also have a person who serves as a patient's rights representative or ombudsman, with the presence and means of contacting this representative described in the handbook given to every patient. While a rights handbook and patient representative should not be limited to record-keeping and data issues, the creation of a data system represents a key occasion for organizations that do not already have such services to bring them into being.

Discussion

The need to inform patients that they have rights and how to exercise them has been recognized by the promulgation of the American Hospital Association's Bill of Rights for Hospital Patients,[18] and similar codes that have been issued recently for special populations, such as nursing home patients,[19] children,[20] and persons who are developmentally disabled.[21] Just what the nature and exercise of these rights should be is the subject of considerable discussion among health-care professionals, consumer and civil liberties groups, and medical organizations, but the importance of such codes is now firmly recognized.

Within organizations creating health data systems, each patient ought to receive a pamphlet or handbook such as the one developed at the Martin Luther King Jr. Health Center. The experience there shows that the very publication of such a patient's rights document helps to orient the staff to its responsibilities and promises, improves patient-staff relationships, and serves as an objective guide for the resolution of disputes that may arise.

The critical element in making patients' rights more than a paper declaration, however, is the presence of an independent patient's rights representative to whom patients can complain or seek help. Such a person must have authority to investigate patient complaints, hold meetings with staff and between staff and patients where this is useful, and to direct staff compliance with the organization's policies where these are found to have been violated.

How to create such a representative and assure his/her independence might be accomplished in various ways. If the organizations' philosophy and top management are fully committed to patient's rights, as at the Martin Luther King Jr. Center, the representative can be an employee of the institution. In the average hospital or health center, there may be problems with an employee exerting independence and enforcing patient rights against medical staffs or administrators. However, trying to overcome that problem by lodging such a function in a government bureau or outside private body has the disadvantage of removing the patient representative from daily in-the-facility availability, which is often critical to the needs of patients. The most promising approach may therefore be to identify the role of patient representative as one that demands independence and advocacy on the part of the person filling it, and using all the available mechanisms of professional and public review to see that primary care institutions permit such representatives to do their jobs in that spirit.

10. The Need for Independent Audit and Periodic Review

Principle

Because the use of EDP by organizations is not a one-time decision as to what will be automated and how, but a continuous process of expanding initial computer applications to additional files, new combinations of data, and more extensive data utilization, (often reflecting new technological resources) any health data system must be subject to regular review by an independent body. Such periodic review should focus not only on the continuing adequacy of the organization's policies and data security in light of changing data processing practices, but also examine any major expansion of the data system that would have significant impact on its treatment of citizen rights.

Discussion

As our description and analysis of computer use in health care has shown, the pace of automation in primary care has begun to accelerate, and major expansion of computer use is predicted in the next decade among hospitals, health centers, doctors' offices, service payer organizations, and quality-care reviewing groups. If projects to develop integrated information systems for hospitals, lifetime patient medical histories, regional planning systems, and similar experiments progress as their proponents believe they will, the late 1970s and early 1980s could be a time of rapid change in the world of health-care computer use.

Projecting this against the essential dynamism of computer applications in organizations, and the pattern of major changes in computer, communications, and optical technologies that have marked these fields during the past two decades, good public policy requires that outside review of an organization's data system not be treated as a one-time certification process. When a hospital installs a computer to process payroll, personnel, patient billing, and lab testing results, it has done something which raises very different issues than when it later automates patient histories and problem-oriented records, joins a regional health planning information system, and decides to send its patient data to an organization like the Multi-State Psychiatric Information System.

For these reasons, periodic review by an outside body ought to be used for all health data systems. As we noted in our discussion of who would conduct such reviews when health data systems were first created, or when public notice and impact statements were first installed as public policy, independent review could be through a private commission or association, a state regulatory agency, or a federal body. Whichever type of review body is chosen, it ought to have rights of inspection, audit, and testing similar to those of an outside financial auditor or professional standards reviewer.

11. The Need to Insure Information for Public Oversight

Principle

There is an inevitable tension between the individual's right of privacy and the public's right to examine and supervise how its social institutions are operating (especially when these are heavily supported by public funds). The rules of confidentiality set by health data systems should be examined carefully to avoid adding to the already existing difficulties in policing compliance with health program requirements and assessing the quality of health care that providers are giving. Using medical records without unique identifiers or with potentially-identifiable data removed represents the major technique for softening the conflict between privacy and public-access interests.

Discussion

The public has already become aware of conflicts between the Federal Privacy Act of 1974 and the newly-amended Federal Freedom of Information Law, and some collision between these two equally valued interests of democratic society must be taken as inevitable, to be resolved (ideally) on a sensitive, situation-by-situation basis.

The problem with health data systems is that the public authorities that are charged with policing fraud and mismanagement, and assuring the quality of care paid for by public funds, are part of the same executive branches (federal, state, and local) whose violations of privacy, confidentiality, and due process have been the subject of anxious public concern during the past decade.

The task of public policy, therefore, is to install statutes or regulations that are so clear as to the uses that can be made of data obtained for public oversight, and have such workable prohibitions and penalties against misuse, that the public can regain confidence in having medical records made available to health-agency personnel. There is also an important need to provide such access for public-interest groups, the media, and other participants in our process of public criticism and review.

Wherever possible, such access should be achieved by techniques such as removing identifiers from records, using special agencies to code and match records that must be assembled from various institutions, and securing the individual's informed consent to use his/her records for such purposes. Where conflicts still arise, judicial review is probably the best resolution. The federal and state courts have shown commendable sensitivity in the past decade in balancing privacy claims and freedom-of-information claims. Their reluctance to accept abstract fears about privacy (often by highly self-interested health-care providers and government payment agencies) and their capacity to work out techniques for making such critical personal records available for public review provide the basis for reasonable optimism in this area.

12. The Importance of Research and Evaluation Using Health Data

Principle

While securing informed, voluntary consent should cover most situations in which medical research and program evaluations need to be conducted, through the use of identified data from health systems, there will be situations in which this is not feasible. In those cases, a health data system should have the purpose, procedures, and safeguards of the research reviewed by a special panel made up of representatives from the organization owning the data system, outside scholars of high reputation, and leaders of public-interest groups relevant to the research project (minority racial groups, womens' groups, civil liberties groups, etc.). Furthermore, securing a legal privilege against any compulsory disclosure of research records should generally be a prerequisite for a health data system's agreement to participate in a research study, disease register, or program evaluation involving highly sensitive personal information.

Discussion

Just as the need for public access to health data must be considered in setting rules for health data systems, there is a similar need to consider how medical research and health-program evaluations will be affected by citizen rights policies.

As we noted in Part One, there has been well-justified criticism of certain research activities in recent years for violating civil liberties. This has included research on dependent or institutionalized people without their knowledge or consent, research that does harm to those on whom it is conducted, research whose procedures violate ethical standards, and research that further stigmatizes various minority groups and cultural dissidents.

Because our study deals with record-keeping and data systems, we noted these issues in Part One only to the extent that they involved the creation and use of personal records. In our report on the impact of computerization, however, we saw that public concern over these types of abusive research activities helped fan public hostility to the creation of some state computerized health data systems for research or evaluation. We also noted that the failure of many such systems to install careful and detailed safeguards against misuse of research data further inflamed the situation.

Recognizing that there is a considerable amount of rational (as well as irrational) "anti-research" sentiment at large today, we must also recognize that the importance of medical research to society and each of its members has probably never been greater than it is today. National health is deeply imperiled by harmful environmental conditions, dangerous foods and drugs in common use, public smoking, substances used at work that produce major diseases among workers, and a variety of other conditions that must be systematically studied and reported upon if public health is to be protected. Further progress in dealing with major killer diseases -- cancer, stroke, and the like -- depends on large-scale research. The relationship of chemical processes to emotional disorders, and their responsiveness to chemical interventions, is another example of prime research. In these and hundreds of other situations, researchers need access to records, usually the identified medical records of people tracked across time and in different medical settings.

There are also important social interests in research to evaluate the effects of health-care programs and systems. The more that concepts of consumer choice, patient responsibility in health management, and new models of health delivery are put forward as alternatives to traditional practices, and the more that public or private funds are spent to underwrite experimental programs along these lines, the more careful and objective evaluations of how these experiments work are needed for decision makers. Precisely because there are such mammoth expenditures at stake, and powerful organizational interests that would be served by continuing the status quo, the forging of political support for enacting new health programs in American society must be followed by commissioning evaluation studies that will test the advantages of the new systems over the old, and identify what may need modification in valuable new programs to correct early defects. The sine qua non of such program evaluation in health care is access to the identified medical records of individuals who participate in such programs, to compare with the experiences of individuals who are receiving different care.

We have taken a moment to spell out the social importance of these research activities because it should remind us that the first concept we presented as a guide for managing ethical data systems is that a democratic society seeks to provide both individual rights and a rationally-ordered social system. These were the twin ideals that men like Jefferson devoted their lives to -- pursuing advances in science and the useful arts to free mankind from the tyranny of nature and help foster the expansion of human liberty.

To carry out that marriage of liberty and reason, health data systems should usually be able to rely on the informed consent of their patients. When long-term research is involved, this will require a different kind of informed consent than the short-term procedure we described earlier, when release of personal data for third parties such as insurance companies, employers, or licensing bodies was involved.

Sometimes, where the research design is known at the time that patients are about to receive treatment or enter a course of care, a full explanation of the uses to be made of personal records can be made and voluntary written consent obtained. Where research projects involve going back to the historical records of patients to trace the effects of certain drugs, medical procedures, health habits, or environmental conditions on the later health status of individuals, reasonable efforts should be made to contact those individuals who are to be studied and to secure their consent; only if this is not possible to do, because the individuals' locations are not available, should consent not be required.

The same initial requirement of informed consent should be used when program evaluations are being done. If evaluations are properly explained, and the safeguards against misuse of identified data are spelled out, most people will cooperate and let their records be used; usually, they will also be glad to supply their experiences and opinions to researchers. The argument that making this voluntary and having non-respondents in samples will throw off the validity of sampling procedures is something that must, ultimately, be considered less important for society than preserving individual rights. Furthermore, analysis of the patterns and reasons for non-response may well be of great importance in judging programs; where such analysis is not feasible, there are still techniques for minimizing distortion of results in such situations.

For the exceptional research situations in which identified records are needed and individual consent cannot be obtained, we suggest the use of special review panels to judge the social importance of the research, the procedures to be followed, the risks to patient privacy that may be involved, and the confidentiality safeguards that will be followed by the researcher. Such panels should be made up of three elements: persons from the organization maintaining the health data system; outside scholars of high professional reputation and experience in serving on ethics committees; and public representatives, especially from groups that may be involved as the subjects of the research (such as blacks, Indians, welfare recipients, women, etc.). Finally, the decisive issue for many health system managers in deciding to authorize a research project may be whether there is an adequate legal privilege available to protect identified records from compulsory production in any investigative, prosecutive, or administrative proceeding by any governmental authority and from production in civil litigation. Statutes providing such privilege have been passed by Congress to cover some executive-designated research projects on alcohol and drug abuse.[22] State privilege laws have also been enacted for some special research, such as Maryland's statute extending total privilege to the data submitted by public and private mental health practitioners to the state psychiatric register.[23]

However, despite arguments in the courts that such a privilege is guaranteed by constitutional rights of privacy, and despite efforts to enact researcher's privilege laws at the state or federal level, the fact is that a general privilege for sensitive research data does not exist today. One solution would be for health professionals, medical societies, and health agency leaders to join civil liberties and media groups in campaigning for such research-privilege laws. But if the complexities of covering the media, general academic research, public-interest research, and medical research all in one statute prove to be insurmountable, then an alternative strategy would be to draft a model law giving legal privilege to medical research by itself. This would be politically promising, since the public's interest in the security of medical research data is great and the justified need to produce it for law enforcement or defendant's rights purposes will arise less often than with media or public-interest research data. If important research utilizing personal information from health data systems is not to be thwarted in the coming decades, installation of such protective legislation must be a high priority for health groups.[24]

C. CURRENT PRIORITIES FOR POLICY ACTION

The work of refining and applying these twelve principles for health data systems is clearly a long-range task. It is already under way in some sectors (as where government health agencies are under fair information practices laws) but there are other areas, primarily in the state and private sectors, in which the job has barely begun.

It was not the assignment of this study to go beyond the presentation and analysis of broad standards to formulate detailed recommendations for policy action. However, our investigation of emerging citizen rights problems in the health field does make it possible to identify an agenda of issues that now seem ripe for action. We will mention examples of issues that require action through legislative, judicial, organizational, and citizen-group initiatives, to stress our conviction that such a mixture of interventions is vital to intelligent policy in the coming years.

1. Legislative Priorities

Some legislative actions involve pin-pointed reforms, in the recognition that society does not think it wise to let these matters be worked out slowly (and uncertainly) through judicial decisions or the fair information practices law route. For example, Congress ought to bring the use of medical information in credit, employment, and insurance reports under the protections of the Fair Credit Reporting Act. One can understand why the legislators in 1970 decided not to include such data when they took their first major step to regulate commercial reporting services, but the record of the past five years has made it plain that consumers deserve to have access rights when medical data is used to deny them credit, insurance, and employment. There are important issues to work out in such an amendment to the 1970 Act, such as whether the individual would see such information directly or have a physician of his choice receive it. But the need to remove the medical exemption from this consumer-protection law flows directly from the principles presented earlier, and nothing presented by industry spokesmen at hearings on this issue is persuasive to the contrary.[25]

Enactment of medical-research privilege laws at the federal and state levels is another specific legislative action that deserves priority treatment. We have already discussed the absence of such legal privilege today and the continual pressures on such data from law enforcement officials, administrators, and other government bodies. A carefully drafted medical-privilege statute ought to command wide professional and public support.

Given the confused and uneven laws in the 50 states on confidentiality of medical information and patient access to records, the development of a model statute and its enactment by as many states as possible would be an important step toward modernizing citizen rights in this area. The American Medical Association has been working on the draft of such a model statute for several years, and their latest version is included in Appendix 3 of this report. While there will be important differences between the AMA and other groups on some aspects of this law, the AMA model bill represents an excellent starting point for discussion. If civil liberties and public interest groups could work cooperatively with the medical profession on refining this measure, and agree to disagree where that is called for, this coalition could provide the driving force for state legislative action. Similar coalitions between civil liberties groups and bankers associations have been important in fighting for privacy of bank records, and a coalition between civil liberties groups and labor unions produced the state laws enacted recently to control compulsory use of polygraphs by employers for hiring and other employment decisions.

With only 5 states having enacted fair information practices laws, anyone concerned with the protection of citizen rights in state, county, and municipal health facilities ought to be pressing their states to join Minnesota, Massachusetts, Utah, Arizona, and New Hampshire in placing government data uses under protective legislation. Indeed, as the Privacy Protection Study Commission holds its hearings in 1976 into the administration of the federal and state privacy acts, and writes its report on the successes and problems that have surfaced thus far with such laws, a stronger and improved model of the Fair Information Practices Law may be developed for other states to adopt.

Finally, explicit citizen rights provisions and a general administrative system that facilitates such rights should be installed in any national health insurance program enacted by Congress. The confidentiality and individual-access policies just enunciated by HEW to govern professional standards review (PSRO) for Medicare and Medicaid are excellent standards, and while there is no experience yet as to how well they will work, these policies could be drawn upon for national health insurance bills and regulations.[26] Many of the principles discussed in this chapter are already in these PSRO policies and could probably be adopted for national health insurance without too much struggle. However, several areas of sharp controversy can be predicted.

While some will see national health records as valuable sources for other social purposes, protection of citizen rights requires that the law have provisions declaring that national health insurance data can be used only for administration and evaluation of the insurance program,and that identified records will not be accessible for any other governmental or private purpose (such as location of deserting fathers, income tax enforcement, police investigations, private lawsuits, etc.)

Some legislators will want to follow the easy path of using the Social Security number for this system, but use of a unique national health insurance number would protect citizen rights by not having medical records include a number that is often known to others and whose presence in these records would facilitate their linkage with other files.

The tendency of many experts designing the administration and data systems of a national health insurance program will be to have summaries of identified records for every participant held in one file in Washington, as Social Security records are now held. They will also want to have patient-identified records of cases on appeal for denial of payment or provider fraud also sent up to regional offices and to Washington. Here too, proper concern for protection of citizen rights should lead to a rejection of such approaches in favor of a system that has identified records kept only at the local level, with the local agency generating a special, randomized review number and removing all unnecessary personal information from any record sent up for review to regional or national offices. Since the provider's identity would be preserved in all records, this ought not to interfere with the audit trails necessary to police against suspected fraud or misconduct.

Finally, some legislators will want to use the "doctor-knows-best" principle to govern an individual's access to his/her record in the national health insurance system. Following the principle already presented in this chapter, we believe that if a medical professional has not been able to convince a patient through personal counseling that direct patient access is unnecessary or unwise, then refusing such access cannot be in the best interests of the patient or consistent with the professional obligation of the physician, and access should be permitted by law.

2. Judicial Actions

Test cases are the accepted way that individuals and groups seek to activate the American state and federal judiciary to advance citizen rights. We have reported quite a few such test-case actions in Chapter 11, and we learned of new ones being filed even as we wrote these concluding remarks.[27] But beyond such specific lawsuits, we think there is a broad strategy that ought to be directed at the courts in the coming years, to establish the common law duty of private organizations and the constitutional duty of government organizations to take reasonable care in the way they handle sensitive personal health data. Where this is set by statute or regulatory order, of course, that would define such a duty and make it enforceable at law. But even in the absence of such laws, we think that there is a failure of legal duty whenever a health data organization does not adopt (a) explicit policies to assure rights of privacy, confidentiality, and individual access; (b) procedures to assure appropriate levels of accuracy, timeliness, and completeness; and (c) adequate data security measures to control improper uses. What constitutes sufficiently explicit policies, appropriate accuracy, or adequate security measures would be defined according to the type of organization and activity involved, and the existing state of the art in data security equipment and techniques. Lawsuits could be brought either by individuals whose interests in privacy and medical care were threatened by organizations using their data without meeting such standards, or by public-interest groups sponsoring class-action suits in the same vein.

It can be argued that setting such standards should be the work of legislation, executive order, or regulatory-agency action, and that invoking the courts is neither responsible public-policy for a democratic society nor a good way to hammer out the detailed rules so often needed. It could also be argued that this would not give organizational managers and computer-systems developers the advance rules they need to avoid ambiguity, and to help justify committing money and staff to the task. Yet the genius of the American judicial system has been its development of new duties for private parties (and redefinition of constitutional rights) to reflect new business activities and technological change. In the common law, this was the way new concepts of contract were developed for mercantile capitalism, and new concepts of tort law for industrialization. Judges today could be equally creative in defining the legal duties of those who use information technology. A failure of duty would be careless and negligent treatment of sensitive personal data, and successful practices would show what is reasonable (and practical) to conduct. After several leading cases had set the main lines of acceptable and unacceptable conduct, the organizational managers and systems developers would have the guidance they sought, and society would have activated an important way of achieving continuing review of organizational responsibility.

3. Organizational Responsibilities

Legislation and judicial decisions take time, and it would be unrealistic to think that many of the priorities just discussed will be installed immediately. This leaves the immediate initiative for action with organizational managers. Furthermore, the standards that will be used by legislators and judges are often drawn from good as well as bad organizational practice in the industry or programs being regulated. This means that the interests of organizational managers in avoiding unwise regulation as well as in the discharge of their own leadership responsibilities makes it important for managements to address such citizen rights issues themselves.

We think any organization maintaining a large-scale data system ought to conduct the kind of serious, in-house "privacy audit" of its principles, policies, practices, and procedures that IBM did in 1974-75; that most federal agencies did in 1975-76 in preparation for complying with the Federal Privacy Act; and that many businesses have been doing in 1976 to see that they are not engaging in controversial practices that would support the enactment of proposed federal measures such as the Koch-Goldwater Bill, H.R. 1984. Such a privacy audit should surface the real problems in the organization; its prime advantage is that it then allows managements--with whatever outside help they may need--to deal with those issues directly and carefully, rather than having the problems accumulate and worsen through management inattention, unfocused data-system decisions, and similar developments.

At the same time, many professional groups have been working recently to formulate new sets of guidelines to deal with citizen rights issues in the health field. These include new guidelines from Blue Shield, the American Society of Internal Medicine, the American Psychiatric Association, community health centers, social workers, nursing home operators, and many others.[28] The concept of creating and legalizing "ethical data centers" that Dr. Elmer Gabrieli and his colleagues have advocated offers another valuable source of guidelines to draw on.[29] The enunciation of such guidelines has played an important role in American society in defining good practice and professional standards, and it deserves to be used to the fullest in extending citizen rights in the health field.

4. Citizen Group Actions

Beyond health-professional organizations, our study has shown that the American Civil Liberties Union has played the single most important role in raising citizen rights issues during the past few years. This has been not only through the activities of the ACLU National Office and its state affiliate chapters, but also through various projects directed or supported by the ACLU, such as the Mental Health Law Project, the Prisoners' Rights Project, the Juvenile Rights Project, and the Project on Privacy and Data Collection. One does not have to agree always with the position taken by an ACLU chapter or the national office to recognize that the continued attention--indeed, the *increased* attention--of ACLU to health-data issues is going to be essential to the working out of good policy in the coming years.

Beyond that, the recent formation of the National Commission on Confidentiality of and Access to Health Care Records is a promising development. Composed of 18 leading organizations in the health field, and growing out of the excellent conference on confidentiality held in Key Biscayne, Florida in late 1974, the Commission could well sponsor just the kind of activities in research, legislative-drafting, consulting, and public testimony that is needed to give coherence and a consensus-forming mechanism to efforts in this area.[30]

Finally, is there any special role to be played by computer professionals in the protection of citizen rights in health care? It can be argued that computer professionals can make their best contribution within the organizations they work for (e.g., hospitals, state health departments, etc.); as private citizens participating in public debates over databank issues; in meetings dealing with medical computing, such as the MEDINFO conventions; or through the general activities of computer groups such as the Association for Computing Machinery, the American Federation of Information Processing Societies, and similar groups. These are all important activities, yet there is an additional one that deserves consideration. When particular government data systems are being considered in local communities or at the state level, whether these are systems in criminal justice, welfare, health, taxation, or other fields, informed computer professionals can do a great deal to help the public interest groups concerned about citizen rights to understand how such proposed systems will work, or how existing systems are working. The computer professionals can also suggest how protections can be worked out within such systems, what the costs are likely to be, and how such systems could be effectively monitered. In addition, whenever public advisory groups or independent audit groups are set up for such data systems, the addition of a citizen-rights oriented computer professional not employed by the government is usually essential to such a group being able to exercise meaningful oversight.

Sometimes computer professionals volunteer for this work or do so as members of the public-interest or civil liberties groups. But the relative infrequency of this professional participation (not only in the health field but in others as well) suggests that we may need some kind of organizational assistance. If the major computer associations, both nationally and through their local chapters, could publicize the availability of volunteer experts to help citizen groups, or to serve on public advisory committees and oversight committees, or to advise legislative committees needing help in sorting out the issues, this might provide the kind of linking mechanism that does not seem to be in place yet in the thousands of local communities and state capitols where the tens of thousands of personal data systems are being built, expanded, and regulated.

CONCLUSION

As American society redefines and reorganizes its health-care system in the coming decade, it will have to make increased use of computer technology to manage the rivers of data that will be generated. Vital medical research, public-health studies, and environmental controls will also require increased reliance on EDP, just as there will be powerful benefits from EDP for individual health care, in the development of permanent patient histories, emergency-treatment communications systems, and similar patient-oriented activities.

If the question is not whether but how such technology will be used in health care, American society has one non-negotiable condition for this process: basic citizen rights cannot be made a casualty of technology-assisted health systems. To do so would be to betray the tradition of Hippocrates, and ultimately to dehumanize health care itself.

It is the custom of Americans to believe that no "lady-or-the-tiger" choice has to be made between science and liberty. For 200 years, in the tradition of Franklin and Jefferson, we have hammered out legal rules that allowed each successive wave of invention to realize its potential, but also required each to be brought under the rule of law. Sometimes it took a while for the principles of regulation to become clear, and we have come to realize that the awesome effects of contemporary technology give us less lead time for social learning and regulatory response than we had in earlier eras. But that is the challenge we face, and there are promising signs that our society understands how important it is to develop, soon, the standards by which we can pursue the benefits of both science and liberty in the field of health care.

FOOTNOTES

1. Lawrence L. Weed, Your Health Care and How To Manage It (Burlington, Vermont: PROMIS Laboratory, 1975).
2. Telephone interview with John Dineen, Health Insurance Association of America, New York City, April 5, 1976.
3. See Part One of this Report for these reactions.
4. The 1975 Guidelines were issued by The National Association of Blue Shield Plans, Chicago, Illinois.
5. Mary Waterstraat and Cynthia H. Stern, "Confidentiality and the Health Insurance Industry, "Paper submitted by the American Medical Record Association, to the Conference on Confidentiality of Health Records, Key Biscayne, Florida, Nov. 6-9, 1974.
6. "Patient Privacy," Psychiatric News, December 5, 1973.
7. Minutes of the ACLU Privacy Committee, February 18, 1976.
8. Murray Weinstock and Jacob I. Haft, "The Effect of Illness on Employment Opportunities," Archives of Environmental Health, Vol. 29, August, 1974, 79-83.
9. Jerry G. Anderson, "A Report on Employee Privacy Within the IBM Corporation," Paper submitted to the Conference on Planning for Action - The Privacy Mandate, sponsored by the U.S. National Bureau of Standards and the Mitre Corporation, April 2-4, 1975.
10. See note 7, supra.
11. Interviews with Dr. John Duffy, Director, IBM Medical Department, 1974 and 1975.
12. Confidentiality: A Guide for Neighborhood Health Centers (Pisani Printing Co., 485 Brannan St., San Francisco, California 94107, 42-44.
13. Simon L. Auster, "Patient Access to Psychiatric Records," Draft Paper, March, 1974.
14. See "Confidentiality," Board of Trustees Report C, February, 1975, American Society of Internal Medicine; Policy of the American Civil Liberties Union on Privacy of Medical Records, 1975; for IBM medical policy, see Anderson, note 9 supra and IBM Medical Manual, in the Appendix of this Report.
15. See the description in Weed, note 1 supra and for the Department of Rehabilitation Medicine, University of Vermont College of Medicine, see Arnold Golodetz, Johanna Ruess, and Raymond Milhous, "The Right To Know: Giving the Patient His Medical Records", Paper presented to the November, 1974 meeting of the American Congress of Rehabilitation Medicine and the American Academy of Physical Medicine; see also "How To Reduce Patient's Anxiety: Show Them Their Hospital Records," Medical World News, January 13, 1975, 48.
16. See Appendix to the Consent Decree in New York State Association for Retarded Citizens v. Rockefeller, April, 1975, available from New York Civil Liberties Union.
17. See Arnold Golodetz, "The Patient and His Medical Record," Paper presented at the Conference on Planning For Action - The Privacy Mandate, sponsored by the U.S. National Bureau of Standards and the Mitre Corporation, April 2-4, 1975, 27-28.
18. Patient Bill of Rights, American Hospital Association, 1972.
19. American Association of Homes for the Aging Bill of Rights, 1974.
20. Medical Bill of Rights for Minors, National Association of Children's Hospitals and Related Institutions, 1974.
21. See the report "Individualized Records for Developmentally Disabled Persons" Task Force on Confidentiality, American Association on Mental Deficiency, Ad Hoc Committee on the Use and Construction of Data Banks, 1974.
22. Comprehensive Drug Abuse and Prevention Act of 1970; Comprehensive Alcohol and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970; Drug Abuse Office and Treatment Act of 1972.
23. Records of Health and Mental Research, Section 101, Art.35, Annotated Code of Maryland.

24. See the proposal for a general researcher's privilege law in Protecting Individual Privacy in Evaluation Research, The Committee on Federal Agency Evaluation Research, Assembly of Behavioral and Social Sciences, National Research Council, National Academy of Sciences, Washington, D.C., 1975.

25. S. 1840 (94th Cong., 1st Sess., 1975) is the bill introduced by Senator William Proxmire to amend the Fair Credit Reporting Act; it includes sections placing medical information under FCRA coverage. For support of this action by the Federal Trade Commission, see Statement of Christian S. White, F.T.C., before the Subcommittee on Consumer Affairs of the Senate Committee on Banking, Housing, and Urban Affairs, Oct. 22, 1975. For opposition by the Retail Credit Corporation (now Equifax), see Statement of W. Lee Burge, Chairman, Retail Credit Company, ibid, October 23, 1975.

26. The PSRO policies are reproduced in Appendix 5.

27. For example, a lawsuit was filed in late April, 1976 attacking the client reporting requirements under Title XX of the Social Security Act by a group of tenants, clinic patients, and legal-aid clients in Connecticut. See Connection, Inc. v. Matthews, United States District Court, District of Connecticut, N-76-94.

28. See the Appendices for the guidelines of Blue Shield and the American Society of Internal Medicine. For the others noted, see Confidentiality and Third Parties, Task Force Report 2, June, 1975, American Psychiatric Association; Confidentiality: A Guide for Neighborhood Health Centers (San Francisco; Pisani Printing Co. 1971); "Information Utilization and Confidentiality" National Association of Social Workers, 1975; Bill of Rights, American Association of Homes for the Aging, 1974.

29. See Appendix 7 for material on the Ethical Data Centers concept.

30. See Confidentiality, Report of the Conference on Confidentiality of Health Records, Key Biscayne, Florida, Nov. 6-9, 1974 (Washington: American Psychiatric Association, 1975).

Selected Bibliography

The following items cover the period through January 1976 and follow the major topical divisions of the Project. Items that are of special importance have been marked with an asterisk (*).

HEALTH CARE: GENERAL

Alford, Robert R., Health Care Politics: Ideological and Interest Group Barriers to Reform, Chicago, University of Chicago Press, 1975.

Alvarez, Rodolfo and Moore, Wilbert E., "Information-Flow Within the Professions: Some Selective Comparisons of Law, Medicine, and Nursing," On Record: Files and Dossiers in American Life, Stanton Wheeler, Editor, New York, Russell Sage Foundation, 1969.

Butler, Patricia, "The Medicaid Program: Current Statutory Requirements and Judicial Interpretations," Clearinghouse Review, May 1974, p. 7.

Commercial Health and Accident Insurance Industry, Hearings Before the Subcommittee on the Judiciary, United States Senate, Ninety-second Congress, Second Session, Parts 1 and 1A, May 10, 11 and June 6,7,8, 1972, Washington, D.C., U.S. Government Printing Office, 1973.

Eisenberg, Barry S., Editor, Socioeconomic Issues of Health, Chicago, Center for Health Services Research and Development, American Medical Association, 1974.

Faxon, Nathaniel, M.D., Editor, The Hospital in Contemporary Life, Cambridge, Harvard University Press, 1949.

Follmann, J.F., Jr., Medical Care and Health Insurance: A Study in Social Progress, Homewood, Illinois, Richard D. Irwin, 1963.

• Freidson, Eliot, Profession of Medicine, New York, Dodd and Mead, 1973.

Fuchs, Victor R., Who Shall Live? Health, Economics, and Social Choice, New York, Basic Books, 1974.

Fulcher, Derick, Medical Care Systems, Geneva, International Labour Office, 1974.

Glaser, William A., Social Settings and Medical Organization, New York, Atherton Press, 1970.

Gold, Don, Bellevue: A Documentary of a Large Metropolitan Hospital, New York, Harper & Row, 1975.

Hicks, Nancy, "Medicare and Medicaid After Decade: A Mixed Picture of Gains and Excesses," New York Times, July 30, 1975, p. 12.

Huffman, Edna K., Medical Record Management, Berwyn, Illinois, Physicians' Record Company, 1972.

Johnson, Sheila K., "Health Maintenance: It Works," New York Times Magazine, April 28, 1974, p. 34.

• Law, Sylvia A., Blue Cross What Went Wrong?, New Haven, Yale University Press, 1974.

Levin, Arthur, M.D., Talk Back To Your Doctor: How To Demand (and Recognize) High Quality Health Care, Garden City, New York, Doubleday & Co., 1975.

Life Insurance Fact Book, New York, Institute of Life Insurance, 1975.

Margolis, Richard J., "Where Does It Hurt? America's Crisis and the Politics of Health Reform," The New Leader, Special Issue, April 15, 1974.

Marmor, Theodore R., The Politics of Medicare, Chicago, Aldine Publishing Company, 1973.

McNabb, Betsy, "Patient Care, Not Proper Care," Southern Hospitals, Vol. 41, April 1973, p. 44.

Murray, D. Stark, Blueprint for Health, New York, Schocken Books, 1974.

Navarro, Vincente, "Health and the Corporate Society," Social Policy, January/February 1975, p. 41.

"Performing Major Surgery on Hospital Costs," Business Week, May 19, 1975, p. 149.

Powell, Mel D., Comprehensive Health Planning: A Manual for Research Officials, Washington, D.C., National Association of Counties Research Foundation.

• Quality Assurance of Medical Care: A Monograph, Papers Presented at a Conference Sponsored by the Regional Medical Program Service, St. Louis, Missouri, January 23-24, 1973.

Schoenrich, Edith H., "Medical Records in Nursing Homes," Maryland State Medical Journal, Vol, 16, August 1967, p. 55.

"The Sky's the Limit on Health Care Costs," *Business Week*, May 26, 1975, p. 72.

Source Book of Health Insurance Data 1974-75, New York, Health Insurance Institute, 1975.

Spiegel, John, *Transactions - The Interplay Between Individual, Family, and Society*, John Papajohn, New York, Science House, 1971.

Stevens, Robert and Stevens, Rosemary, *Welfare Medicine in America: A Case Study of Medicaid*, New York, The Free Press, 1974.

Turner, E.S., *Call the Doctor: A Social History of Medical Men*, London, Michael Joseph, 1958.

U.S. Department of Health, Education and Welfare, *Health of the American Indian*, Washington, D. C., U.S. Government Printing Office, April 1973.

U.S. Department of Health, Education and Welfare, *PSRO Program Manual*, reprinted by the American Hospital Association, Chicago, 1974.

Vital and Health Statistics Programs and Collection Procedures, "Development and Maintenance of a National Inventory of Hospitals and Institutions," Washington, D.C., U.S. Department of Health, Education and Welfare, Public Health Service, 1965.

Warner, Judith and Aherne, Phil, Editors, *Profile of Medical Practice*, Chicago, Center for Health Services Research and Development, American Medical Association, 1974.

HEALTH-CARE RECORD-KEEPING: GENERAL

* Acheson, E.D., *Medical Record Linkage*, New York, Oxford University Press, 1967.

American Medical Record Association, "An Instruction Guide for Organizing Health Records," 1974.

Bernstein, Arthur H., "Examining and Using Hospital Records," *Hospitals*, Vol. 43, October 1, 1969, p. 86.

Bernstein, Arthur H., "Medical Record Contents: Incident Report in the Medical Record of the Patient," *Hospitals*, Vol. 39, August 1, 1965, p. 28.

Bowden, Lois, "Social Security Numbers for Patient Identification," *Hospitals*, Vol. 46, April 1, 1972, p. 14.

Bredenberg, Viola C., "Providing Patient Diagnosis to Regular Visiting Clergy," *Hospital Progress*, Vol. 49, April 1968, p. 64.

Brown, Murray C., "V.D.: Medical Records Play Major Role in Campaign to Control Epidemic," *Medical Record News*, Vol. 43, October 1972, p. 67.

Brzica, S.M. and Lesler, J.L., "The Use and Disclosure of Medical Information Submitted for Social Security Disability Purposes," *South Dakota Journal of Medicine*, Vol. 24, September 1971, p. 20.

Collins, M. Clagett and Ballard, James O., "Capturing the Physician's Thought Processes: The Problem Oriented Medical Record," *New Physician*, Vol. 22, October 1973, p. 626.

* *Conference on Neighborhood Health Center Records*, sponsored by the Intermountain Regional Medical Program in cooperation with the American Medical Record Association Salt Lake City, Utah, March 18-20, 1971.

Converse, Mary E., "Geriatric Medical Records," *Hospitals*, Vol. 39, April 16, 1965, p. 34.

Converse, Mary E., "Retention of Medical Records," *Hospitals*, Vol. 44, May 1, 1970, p. 16.

Converse, Mary E., "What Nonmedical Information Should Be Filed with a Patient's Medical Record?" *Hospitals*, Vol. 43, June 16, 1969, p. 52.

"Description of the Client Information System," State of Michigan, Department of Social Services, November 1973.

Deshaies, John C., "Census Use Study, Report No. 7: Health Information System," Washington, D.C., U.S. Department of Commerce, Bureau of the Census, 1969.

Desk Reference on Drug Abuse, Chicago, American Hospital Association, 1970.

"Disposition of Patient's Records," New York Medicine, Vol. 26, August 1970, p.329.

• Erikson, Kai T. and Gilbertson, Daniel E., "Case Records in the Mental Hospital," in Stanton Wheeler, Editor, On Record: Files and Dossiers in American Life, New York, Russell Sage Foundation, 1969.

Esley, Carole E., RRA, "Implementing the POMR System: Guidelines for Medical Record Personnel," Medical Record News, February 1973, p. 33.

Essentials of Social Work Programs in Hospitals, Chicago, American Hospital Association, 1971.

Finnegan, Rita, "Outpatient Medical Records - The Future," Medical Record News, Vol. 41, August 1970, p. 11.

Forkner, C. E., "Better Medical Records," Bulletin of the American College of Physicians, Vol. 11, June 1970, p. 284.

Gay, Lorraine G., "International Study Project on Record Linkage in Community Health and Hospital Services," Medical Record News, August 1972, p. 34.

Geller, E. I., "Personal Medical Retrieval System," Journal of Occupational Medicine, Vol. 13, July 1971, p. 353.

• Gertzog, Jack, "The Changing Concept of Medical Records," Medical Record News, Vol. 42, June 1971, p. 11.

Givens, Lois, "Medical Record Circulation Control System," Medical Record News, Vol. 43, February 1972, p. 39.

Gordon, Burgess, Methodology for the Preparation of Medical Records, Presentation on Medical Terminology at the Tenth International Congress on Diseases of the Chest, Washington, D.C., October 4-8, 1968.

Gordon, Burgess, "Preciseness and Specificity for Medical Records," Journal of the American Medical Association, Vol. 197, August 15, 1966, p. 569.

Gordon, Burgess, "Regularization and Stylization of Medical Records," Journal of the American Medical Association, Vol. 212, June 1, 1970, p. 1502.

Hall, George, "Student Health Record," Journal of the American Medical Association, Vol. 192, May 10, 1965, p. 560.

Herr, Conrad E., M.D., and Patrikas, Elaine O., "Documentation of Hospital Based Ambulatory Care," Hospitals, March 1975.

"History and Organization of the Vital Statistics System," Vital Statistics of the United States, U.S. Department of Health, Education and Welfare, Public Health Service, National Vital Statistics Division, 1950.

Horiuchi, Helen S., "Bibliography on Record Linkage," Medical Record News, August 1972, p. 66.

Hospital Accreditation Program, Accreditation Manual for Hospitals, Chicago, Joint Commission for Accreditation of Hospitals, 1970.

• Hospital Medical Records: Guidelines for Their Use and the Release of Medical Information, Chicago, American Hospital Association, 1972.

Hoyt, Emmanuel and Hoyt, Jonathan, Legal Aspects of Medical Records, Berwyn, Illinois, Physician's Record Company, 1964.

• Huffman, Edna K., Manual for Medical Record Librarians, Berwyn, Illinois, Physicians' Record Company, 1972.

"International Study Project on Record Linkage in Community Health and Hospital Services," Chicago, American Medical Record Association, 1972.

• Keller, Martin D., "The Patient, the System, and the Record: How Are They Doing Doctor?" Quality Assurance of Medical Care, Regional Medical Programs Service, Health Services and Mental Health Administration, U.S. Department of Health, Education and Welfare, February 1973.

Kirby, William H., "Secondary Users of Clinical Records: An Overview," Journal of Clinical Computing, Vol. 3, September 1973, p. 153.

Laird, Onalee M., "Medical Records," Hospitals, Vol. 40, April 1, 1966, p. 109.

Laird, Onalee M., "Medical Records," Hospitals, Vol. 43, April 1, 1969, p. 153.

Levey, Samuel and Loomba, N. Paul, Health Care Administration, A Managerial Perspective, Philadelphia, J.B. Lippincott, 1973.

MacEachern, Malcolm T., *Hospital Organization and Management*, Chicago, Physician's Record Company, 1957.

• MacEachern, Malcolm T., *Medical Records in the Hospital*, Chicago, Physician's Record Company, 1937.

Manes, Rose T., RRA, "Medical Record Personnel; Does the Supply Meet the Demand," Medical Record Association of New York State, 1975.

Mangold, William J. Jr., "The Importance of Adequate Record-Keeping," *New Physician*, Vol. 22, April 1973, p. 239.

"Maryland Psychiatric Case Register: Description of History, Current Status and Future Use," Maryland Department of Mental Hygiene and N.I.M.H., December 1967.

McDonald, Pat, "An Intra-Institutional Linkage System," *Medical Record News*, August 1972, p. 39.

McNamara, Evelyn M., "Should A Social Work Record Be Included in a Patient's Medical Record?" *Hospitals*, Vol. 47, September 16, 1973, p. 12.

• *Medical Record Departments in Hospitals: Guide to Organization*, Chicago, American Hospital Association, 1972.

"Medical Record Services," *Accreditation Manual for Hospitals*, Joint Commission on Accreditation of Hospitals, 1970, updated 1973, p. 105.

Medical Records Practice in New Zealand, New Zealand National Health Statistics Centre, Department of Health, 1974.

"More on Wallet-Size Medical Histories," *Medical World News*, Vol. 13, March 24, 1972, p. 46.

Murnaghan, Jane H., Editor, *Ambulatory Care Data: Report of the Conference on Ambulatory Medical Care Records*, Sponsored by National Center for Health Services Research and Development, National Center for Health Statistics, The Johns Hopkins University, J. B. Lippincott Company, 1973.

Nahmias, A. J. and J. E. McCroan, "A Community Surveillance System of Infectious Diseases in the Greater Atlanta Area," *American Journal of Public Health*, Vol. 56, March 1966, p. 408.

National Center for Health Statistics, Health Services and Mental Health Administration, Public Health Service, U.S. Department of Health, Education and Welfare, *Proceedings of the Public Health Conference on Records and Statistics*, June 17-21, 1968, Washington, D. C., U.S. Government Printing Office, 1968.

National Center for Health Statistics, Health Services and Mental Health Administration, Public Health Service, U.S. Department of Health, Education and Welfare, *Proceedings of the Public Health Conference on Records and Statistics*, June 12-15, 1972, Washington, D.C., U.S. Government Printing Office, 1973.

National Center for Health Statistics, Health Services and Mental Health Administration, Public Health Service, U.S. Department of Health, Education and Welfare, *Use of Vital and Health Statistics in Epidemiological Research: A Report of the United States National Committee on Vital and Health Statistics*, Washington, D.C., U.S. Government Printing Office, 1968.

National Center for Health Statistics, *Origin, Program, and Operation of the U.S. National Health Survey: Vital and Health Statistics*, Washington, D.C., U.S. Government Printing Office, April 1965.

Nemec, Frances C., "Useful Medical Record System for a Decentralized Mental Hospital," *Hospital and Community Psychiatry*, Vol. 17, October 1966, p. 312.

"New Records System for Psychiatric Hospitals," *Public Health Reports*, Vol. 82, September 1967, p. 832.

Patrikas, Elaine O., RRA, "Problem Oriented Medical Record: Some Implications for Medical Record Administration," *Journal of Clinical Computing*, Fall 1973.

Peterson, Osler L., "An Analytical Study of North Carolina General Practice," *Journal of Medical Education*, Vol. 31, December 1956, p. 23.

"Physician and Hospital Records Retention and Inspection," *Wisconsin Medical Journal*, Vol. 72, January 1973, p. 43.

Plasman, F. Boiten, "The Medical Record--The Basis for an Automated Information System," *Medical Record News*, June 1972, p. 15.

Puder, Barbara, RRA, "The Unit Data System," *Medical Record News*, October 1975, p. 59.

Rogers, T.V. and Clark, M.E., "Sharing Information by Means of the Patient's Medical Record," *Journal of the American Dietetic Association*, Vol. 63, July 1973, p. 43.

Shapiro, Sam, "Production of Uniform Data for Health Care Plans," *New England Journal of Medicine*, Vol. 288, June 28, 1973, p. 1407.

Task Group on Uniform Use of Medical Terms and Code, *Coordinated Planning of a Health Information System*, Buffalo, New York, Clinical Information Center, E. J. Meyer Memorial Hospital, June 3, 1969.

* *The Problem Oriented Medical Record - A Special Collection of Selected Articles*, American Medical Record Association, Chicago, Illinois, October 1971.

U.S. Department of Health, Education and Welfare, Social Security Administration, *Social Security Programs in the United States*, Washington, D. C., U.S. Government Printing Office, 1973.

United States National Committee on Vital and Health Statistics, "Use of Hospital Data for Epidemiologic and Medical-Care Research," Washington, D.C., United States Department of Health, Education and Welfare, Public Health Service, Health Services and Mental Health Administration, 1969.

Vital Health and Statistics Programs and Collection Procedures, "Health Survey Procedure," Washington, D.C., United States Department of Health, Education and Welfare, Public Health Service, 1964.

Von Edmond, J. and Wieme, R., "Coding Diagnoses of Medical Records,"*Journal of Clinical Computing*, Vol. 3, September 1973, p. 130.

Von Hoek, Robert and Scolsey, Theodore, "Uniform Basic Data Sets: A Tool for Improving Health Care Delivery," *Medical Record News*, Vol. 44, February 1973,p. 16.

* Weed, Lawrence L., *Medical Records, Medical Education, and Patient Care*, Chicago, Year Book Medical Publishers, 1971.

Weed, Lawrence L., "Medical Records That Guide and Teach," *New England Journal of Medicine*, Vol. 278, March 14, 1968, p. 593, and March 21, 1968, p. 652.

Weed, Lawrence L., "Quality Control and the Medical Record," *Archives of Internal Medicine*, Vol. 127, January 1971, p. 101.

Wheeler, Stanton, Editor, *On Record: Files and Dossiers in American Life*, New York, Russell Sage Foundation, 1969.

* Wilberding, Joseph C., "The Medical Information Bureau," *Transactions and Studies of the College of Physicians of Philadelphia*, Vol. 37, July 1969, p. 43.

COMPUTER APPLICATIONS IN HEALTH CARE

"A Mental Patient's Rights to Adequate Care Upheld," *New York Times*, November 9, 1974, p. 34.

"A Review of Automated Multiphasic Health Testing Centers," *Hospitals*, Vol. 45, March 1, 1971.

"A Wallet-Size Medical History," *Medical World News*, Vol. 13, February 11, 1972,p.5.

Allen, C.M., M.D., and Shinefield, H.R., M.D., "Automated Multiphasic Screening," *Pediatrics*, November 1974, p. 621.

Altman, Lawrence K., "Computers Urged As Aid to Doctors," *New York Times*, December 11, 1970, p. 31.

* Anderson, J. "Kings Hospital Computer System (London)," in Morris F. Collen, Editor, *Hospital Computer Systems*, New York, John Wiley and Sons, 1974.

* Anderson, J. and Forsythe, J.M., *Medinfo 74*, First World Conference on Medical Informatics, Stockholm, Sweden, August 5-10, 1974, Preprints of Papers.

Anderson, Odin W., "Medical Technology and the Political System," *Technology and Health Care Systems in the 1980's*, Morris F. Collen, Editor, Proceedings of a Conference, San Francisco, California, January 19-21, 1972, National Center for Health Services Research and Development, Health Services and Mental Health Administration, U.S. Department of Health, Education and Welfare, 1972.

Antley, Ray M., M.D., and Antley, MaryAnn, M.A., "Automation: Its Impact on the Delivery of Health Care," *Computers and Automation*, April 1973, p. 11.

Antley, Ray M., M.D., and Antley, Mary Ann, M.A., "Changing Technology and Medical Specialization, " *Computers and People*, December 1974, p. 15.

Ashford, J. R. and Pearson, N. G., "The Exeter Community Health Research Project," *Computers in the Service of Medicine, Vol. 1*, G. McLachlen and R.A. Shegog, Editors, London, Oxford University Press, 1968.

* *Automation and Data Processing in Psychiatry*, A Report of a Task Force of the American Psychiatric Association on Automation and Data Processing, Washington, D.C., March 1971.

"Automated Medical Information System To Be Instituted in Southern Arizona," *Arizona Medicine*, Vol. 25, September 1968, p. 820.

Baird, Henry W. and Garfunkel, Joseph M., "Electronic Data Processing of Medical Records," *New England Journal of Medicine*, Vol. 272, June 10, 1965, p. 1211.

* Ball, M.J., "Medical Data Processing in the United States," Proceedings of the 1974 National Computer Conference and Exposition, Chicago, May 6-10, 1974, AFIPS Press, Vol. 43, p. 215.

Ball, Marion J., "Computers: Prescription for Hospital Ills," *Datamation*, September 1975, p. 50.

Baloff, Nicholas; Hershey, John C.; and Moore, John R.; "An Integrated Health Services Data System," Research Paper No. 106, Stanford University, Graduate School of Business, 1972.

Barnes, J.L., "92 - Bed Hospital Finds It Is 'Big Enough' for Its Own In-House Computing System," *Medical Record News*, Vol. 44, April 1973, p. 19.

* Barnett, G.O., "Massachusetts General Hospital Computer System (Boston)," in Morris F. Collen, Editor, *Hospital Computer Systems*, New York, John Wiley & Sons, 1974.

Barnett, G.O., "Technology and Productivity in the Health Field," *Application of Technology To Improve Productivity in the Service Sector of the National Economy*, National Academy of Engineering, 1973.

Bauer, Katharine G. and Joroff, Michael L., *Toward A Comprehensive Community Health Information System*, Prepared for Meeting of Urban and Regional Systems Association, September 1969.

* Bauman, William Allen, "Inpatient Information System," *New York State Journal of Medicine*, Vol. 73, September 15, 1973, p. 2248.

* Baxter, Edward, et al., "An Evaluation of (Medical Record) Recording Systems," *Hospitals*, Vol. 45, December 16, 1971, p. 72.

Beggs-Baker, Susan, "Evaluation Method: The Experience ofthe Casa de Amigos Computerized Patient Management System," in Koza, Russell C., *Health Information Systems Evaluation*, Boulder, Colorado, Colorado Associated University Press, 1974, p. 115.

Beggs-Baker, Susan, et al., "Evaluation of a System for On-line Computer Scheduling of Patient Care Activities," *Computers and Biomedical Research*, Vol. 4, 1971,p.634.

Bekey, George A. and Schwartz, Morton D., Editors, *Hospital Information Systems*, Marcel Dekker, 1972.

Bemer, R.W., Editor, *Computers and Crisis: How Computers Are Shaping Our Future*, Association for Computing Machinery, 1971.

* Bennett, W. L., "The Computer and the Clinician," *Medinfo 74*, J. Anderson and J.M. Forsythe, Editors, First World Conference on Medical Informatics, Stockholm, Sweden, August 5-10, 1974.

Berry, Charles A., "The Impact of Emerging Technology on Health Care Systems," *Technology and Health Care Systems in the 1980's*, Morris F. Collen, Editor, Proceedings of a Conference, San Francisco, California, January 19-21, 1972, National Center for Health Services Research and Development, Health Services And Mental Health Administration, U.S. Department of Health, Education and Welfare, 1972.

Bise, B.W., "A Resource Allocation and Planning System for the Development and Operation of Health Care Delivery Systems," Proceedings of the 1974 National Computer Conference and Exposition, Chicago, May 6-10, 1974, AFIPS Press, Vol. 43, p. 207.

* Bonner, Paul A., "Data Processing Systems for Medical Care Appraisal," *PSRO: Organization for Regional Peer Review*, Barry Decker and Paul Bonner, Editors, Ballinger Publishing Company, 1973.

Bottinger, Lar Erik, "The Evolving Swedish Health Data System," Excerpt from *Transactions of the Conference held by the Center for Continuing Medical Education*, E.R. Gabrielli, Editor, Buffalo, June 3-6, 1971.

Branch, Charles D., M.D., "Age of the Computer in Patient Care," *The American Journal of Surgery*, November 1974, p. 638.

Breasted, Mary, "9-Hospital Link To Fight Cancer," *New York Times*, November 2, 1975, p. 38.

Brody, Jane E., "3-Dimensional X-Ray Is Tested for New View of Body," *New York Times*, October 22, 1975, p. 89.

Brungard, W. Robert, "Accounting System Increases Cash Flow by $500,000 at Community Hospital, *Computerworld*, January 12, 1976, p. 34.

Buckley, J. D.; Gledhill, V.X.; Mathews, J.D.; and Mackay, I.R.; "A Computer Based Medical Record System," *Methods of Information in Medicine*, Vol. 12, July 1973, p. 137.

Bumbalo, Thomas S., "Community Health Information," *Computerization of Clinical Records*, E.R. Gabrieli, Editor, New York, Grune and Stratton, 1970.

Butkus, Charles, "System Cuts Medicaid Processing to 11 Cents a Claim," *Computerworld*, May 21, 1975, p. 51.

Caceres, Cesar A.; Weihrer, Anna Lea; and Pulliam, Robert; "Information Science Applications in Medicine,"in Cuadra, Carlos A., Editor, *Annual Review of Information Science and Technology*, Volume 6, Chicago, Encyclopedia Britannica, 1971, p. 325.

Ceransky, Walter A. and Haynes, Ernest R., "A Record and Filing System for Family Practice," in E.R. Gabrieli, Editor, *Computerization of Clinical Records*, New York, Grune and Stratton, 1970.

"Certified Records Managers Institute Formed, Certification Procedures Set," *Government Data Systems*, July/August, 1975, p. 6.

Chalice, R.; Haring, O.H.; and Hochsprung, R.; "Automated Patient Record Summaries for Health Care Auditing,"*Proceedings of the 1974 National Computer Conference and Exposition*, Chicago, May 6-10, 1974, AFIPS Press, Vol. 43, p. 81.

* Collen, M., "Automated Multiphasic Health Testing," in Morris F. Collen, Editor, *Hospital Computer Systems*, New York, John Wiley & Sons, 1974.

* Collen, M., "General Requirements," in Morris F. Collen, Editor, *Hospital Computer Systems*, New York, John Wiley & Sons, 1974.

* Collen, Morris F., Editor, *Hospital Computer Systems*, New York, John Wiley & Sons, 1974.

* Collen, Morris, F., *Medical Information Systems*, Health Services and Mental Health Administration, Public Health Service, U.S. Department of Health, Education and Welfare, January 28-30, 1970.

Comprehensive Psychiatry, Special Issue, Psychiatry and the Computer, Vol. 8, December 1967.

Computer Applications in the Field of Medicine, Rome, Sperry/Univac International Executive Centre, 1970.

Computer Applications in the Juvenile Justice System, Proceedings of the National Symposium on Computer Applications in the Juvenile Justice System, Atlanta, Georgia, December 6-8, 1973, Reno, Nevada, National Council of Juvenile Court Judges, 1974.

"Computer Speeds Clinic's Service," *New York Times*, December 26, 1970, p. 23.

"Computers in Medicine: Hospitals Cope with Costs, Quality Review," *Science*, February 28, 1975, p. 730.

"Confidentiality and Security--Numerous Approaches," *Computers and Medicine*, May/June 1973.

Cook, Margo, "Introduction of a User-oriented THIS into a Community Hospital Setting - Nursing," *Medinfo 74*, *op. cit.*

Cordle, Frank, "The Automation of Clinical Records," *Medical Care*, Vol. 10, November-December 1972, p. 470.

* Crawford, Jeffrey L., "Computer Applications in Mental Health: A Review," in Jeffrey L. Crawford, Donald W. Morgan and Daniel T. Gianturco, Editors, *Progress in Mental Health Information Systems: Computer Applications*, Cambridge, Massachusetts, Ballinger Publishing Company, 1974.

• Crawford, Jeffrey L.; Morgan, Donald W. and Gianturco, Daniel T.; Editors, *Progress in Mental Health Information Systems: Computer Applications*, Cambridge, Massachusetts, Ballinger Publishing Company, 1974.

Crawford, M., "Medical College of Georgia: Computerized Patient Information System," *Medical Record News*, Vol. 40, October 1969, p. 34.

• Crooks, J., "Computer Applications in Patient Follow-Up," in G. McLachlan and R.A. Shegog, Editors, *Computers in the Service of Medicine*, Volume I, London, Oxford University Press, 1968.

• Cross, K.W.; Droar, J. and Roberts, J.L.: "Electronic Processing of Hospital Records," in McLachlan and Shegog, *Computers in the Service of Medicine, Vol. I*.

• Dale, J.W. and Roberts, J.L., "The Identification of Patients and Their Records in a Hospital Using Electronic Data-Processing Equipment," in McLachlan and Shegog, *Computers in the Service of Medicine, Vol. I*.

"Data Banks and Hospitals," *Datamation*, Vol. 15, March 1969, p. 129.

"Data Security and Data Processing, Volume 4, Study Results: Massachusetts Institute of Technology"(IBM Corporation).

Davidson, Ronald G., "Record Linkage and Genetics," in E.R. Gabrieli, *Computerization of Clinical Records*.

• Davis, L., "Data Processing Facilities," in Morris F. Collen, *Hospital Computer Systems*.

• Davis, L. and Terdiman, J., "The Medical Data Base," in Morris F. Collen, *Hospital Computer Systems*.

• Davis, Lou S., "A System Approach to Medical Information," *Methods of Information in Medicine*, January 1973, p. 1.

• Davis, Lou S., "Data Security Considerations in a Medical Data System," Oakland, California, Kaiser-Permanente Medical Care Program, March 30, 1973.

Davis, Ruth M., "Technology, A Discontinuity in Our Society," in *Technology and Health Care Systems in the 1980's*, *op. cit.*

"Dedicated System Produces Reports as By-Products," *Computerworld*, January 26, 1976, p. S/11.

DeDombal, F.T. and Horrocks, Jane C., "Computer-aided Diagnosis: Conclusions from an Overall Experience Involving 4469 Patients," *Medinfo 74*, *op. cit.*

• DeLand, E.C. and Waxman, B.D., *Review of Hospital Information Systems*, Rand Corporation, June 1970.

"Demythologizing Medicine, or, How to Stop Worrying and Love the Computer," *Journal of the American Medical Association*, May 5, 1975, p. 515.

Devine, Bob, "Prospective Medicine: A Health Forecast," *Pastimes*, December 1974, p. 15.

Dinsdale, Sidney M. et al., "Problem Oriented Medical Records: Their Impact on Staff Communication, Attitudes and Decision Making," *Archives of Physical Medicine and Rehabilitation*, Vol. 56, June 1975, p. 269.

Donahoe, Alice M., "Computer System Provides Flexible Control of Medical Records," *Hospitals*, Vol. 47, June 16, 1973, p. 116.

"DP Proves Useful Tool in Search for Medicaid Abuses," *Computerworld*, December 30, 1970/January 6, 1971, p. 6.

Drug Research Board of the National Academy of Sciences-National Research Council, *Report of the International Conference on Adverse Reactions Reporting Systems*, October 22-23, 1970, Washington, D.C., 1971.

Dunn, Halbert L., "Record Linkage," *American Journal of Public Health*, Vol. 36, December 1946, p. 1412.

EDP for Hospitals - New Directions for Survival, New York, Quantum Science Corporation.

Eiduscon, B.T., "An Approach to Retrieval of Narrative Text in Case Records: The Psychiatric Case History Event System (PsyCHES)," *Methods of Information in Medicine*, Vol. 9, October 1970, p. 201.

Elinson, J. and Colombotos, J., *Physicians' Attitudes Towards Automated Multiphasic Health Screening, Final Report for Project HSM-110-69-238*, New York, Columbia University, June 1972.

Ellwood, Paul M., et al., Information Systems for Comprehensive Health Planning, Minneapolis, Minnesota, The American Rehabilitation Foundation, 1967.

Enkelis, Myra, Systems Concepts and Data Processing Methods: An Introduction, Chicago, American Association of Medical Record Librarians, 1968.

Enslein, Kurt and Pixley, David C., "Design of Computer-Compatible Records System," in E.R. Gabrieli, Computerization of Medical Records.

• Ertel, Paul Y., "Automated Review of Professional Services and the Problems of Medical Records," Journal of Clinical Computing, Vol. 3, September 1973, p. 177.

• Findikyan, Nyrhan; Laska, Eugene M.; and Bank, Rheta; "A Review of the Multi-State Information System for Psychiatric Patients," Medinfo 74, op. cit.

Fisher, George F., et al.,"'Do-It-Yourself' Computer Reports in the Medical Record Department," Medical Record News, Vol. 43, June 1972, p. 31.

Flagle, Charles D., "Evaluation and Control of Technology in Health Services," in Technology and Health Care Systems in the 1980's, op. cit.

• Flagle, C. "Operations Research with Hospital Computer Systems," in Morris F. Collen Hospital Computer Systems.

Fowler, D. Robert, M.D. and Longabaugh, Richard, Ed.D., "The Problem-Oriented Record," Archives of General Psychiatry, July 1975, p. 831.

Frank, Ronald A., "Medical Field Ill-Prepared for First DP Encounters," Computerworld, August 14, 1974, p. 1.

• Freibrun, R. B., "Effective Planning for and Justification of the Extension of Data Processing in Hospitals," Proceedings of the 1974 National Computer Conference and Exposition, Chicago, May 6-10, 1974, AFIPS Press, Vol. 43, p. 201.

French, Nancy, "Inadequate Automation Cited as Health System's Flaw," Computerworld, June 4, 1975, p. 26.

French, Nancy, "Mini System Orders Medical Tests, Relays Results," Computerworld, January 26, 1976, p. S/8.

French, Nancy, "Report Highlights Industries with Large DP Growth Potential," Computerworld. November 19, 1975, p. 45.

French, Nancy, "Retrieval System Developed In-House Speeds Claims," Computerworld, February 12, 1975, p. 9.

French, Nancy, "Use of Minis in Government Doubled Between '67, '74," Computerworld, December 3, 1975, p. 33.

Fries, James F., "Times - Oriented Patient Records and a Computer Databank," Journal ofthe American Medical Association, Vol. 222, December 18, 1972, p. 1536.

• Gabrieli, E. R., "Automation of Discharge Summary in the Hospital," in E.R. Gabrieli, Computerization of Medical Records.

Gabrieli, E. R., "Clinical Aspects of Machine-Compatible Record Designing," Transactions of the Conference on the Use of Computers in Clinical Medicine, Buffalo, New York, October 2-5, 1969.

Gabrieli, E. R., "Clinical Medicine and Fundamentals of Human Communication," in E. R. Gabrielli, Computerization of Medical Records.

• Gabrieli, E. R., Editor, Clinically Oriented Documentation of Laboratory Data, New York, Academic Press, 1972.

Gabrieli, E. R., "Computers and the Medical Data Bank," New Physician, Vol. 19, February 1970, p. 148.

Gabrieli, E. R., M.D., Computerization of Clinical Records, Vol. I, New York, Grune and Stratton, 1970.

• Gabrieli, E. R., "Concept of an Area-Wide Health Data Network,"in E. R. Gabrieli, Computerization of Medical Records.

Gabrieli, E. R., "Medical Network," Datamation, October 15, 1970, p. 42.

Gabrieli, E. R., Editor, Planning a Health Information System, Buffalo, State University of New York at Buffalo.

Gabrieli, E. R., "Standardization of Medical Documentation," Datamation, August 1969, p. 103.

• Gabrieli, E. R.; Nagy, Emil J.; and Williams, Wilson, L.; "Clinical Applications of Systems Analysis and Systems Design: Principles of Computer-Compatible Logic," Conference on Use of Computers in Clinical Medicine, Buffalo, October 2-5, 1969.

Gall, J. E., Jr., "Introduction of a User-Oriented THIS into a Community Hospital Setting - Tactical Management Revelations," *Medinfo 74*, *op. cit.*

Garfield, J. and Dafra, I.R., "A Computer and Physician Acceptable Medical Record for a Chest Service," Conference on the Use of Computers in Clinical Medicine, Buffalo, October 2-5, 1969.

* Garfield, S., "The Computer and New Health Care Systems," in Morris F. Collen, *Hospital Computer Systems*.

Garfield, S. R., "A New Ambulatory Health Care Delivery System Model," *Medinfo 74*, *op. cit.*

Garvin, Richard L., "Impact of Information-handling Systems on Quality and Access to Health Care," *Public Health Reports*, Vol. 83, May 1968, p. 345.

Gay, Lorraine G., "Summary and Comment on Four U.S.A. Linkage Systems," Speech Prepared for Delivery at the Sixth International Congress on Medical Records, *Medical Record News*, August 1972, p. 34.

Gay, Lorraine,"The VA Patient Treatment File," *Medical Record News*, August 1972, p. 58.

* Gianturco, Daniel T. and Ramm, Dietolf, "Computer Aided Patient Evaluation: A Goal Oriented Approach,"in Jeffrey L. Crawford et al., *Progress in Mental Health Information Systems: Computer Applications*.

* Giebink, Gerald A. and Hurst, Leonard L., *Computer Projects in Health Care*, Ann Arbor, Michigan, Health Administration Press, University of Michigan, 1975.

Glaser, Jay H., "Health Information Systems: A Crisis or Just More of the Usual," *American Journal of Public Health*, Vol. 61, 1971, p. 1524.

*Glueck, Bernard C., "Computers at the Institute of the Living," in Jeffrey L. Crawford et al., *Progress in Mental Health Information Systems:Computer Applications*.

"The Great Medicaid Scandal," *Time*, May 26, 1975, p. 55.

* Grossman, Jerome H. et al., "An Automated Medical Record System," *Journal of the American Medical Association*, Vol. 224, June 18, 1973.

* Hall, P. "Karolinska Hospital Computer System (Stockholm)," in Morris F. Collen, *Hospital Computer Systems*.

Hall, P.; Mellner, Ch.; and Danielsson, T.; "A Data Processing System for Medical Information," *Methods of Information in Medicine*, Vol. 6, January 1967, p. 1.

Hallen, B.; Mellner, Ch.; Selander, H; and Wolodarski, J; "Gudelines for Choice of Anaesthesia - A Result of the Computerized Patient Data Base at the Karolinska Hospital," *Medinfo 74*, *op. cit.*

Harding-Smith, R.H., "Cost Effectiveness for Decision Taking and Evaluation," *Conference on Computer Applications in the Field of Medicine*, Rome, Sperry-Univac International Executive Centre, April 2-4, 1974.

Harmon, Leon D., "Some Problems and Priorities in Health Care Technology," in *Technology and Health Care Systems in the 1980's*, *op. cit.*

Hawkins, R. E., "Introduction of a User-Oriented THIS into a Community Hospital Setting - Introductory Agents and Their Roles," *Medinfo 74*, *op. cit.*

Haynes, Alfred, "Health Care, Technology and the Social System," *Technology and Health Care Systems in the 1980's*, *op. cit.*

"Health and Welfare Management Systems: The Years of Transition," *Government Data Systems*, May-June 1974.

Hebert, John, "Source Data Entry Eases Patient Admissions Process," *Computerworld*, October 29, 1975, p. S/13.

Hellman, J.J., *Privacy and Information Systems: An Argument and an Implementation*, The Rand Corporation, May 1970.

Hempenius, K. amd Scholtis, R.J.H., "The Real-Time Computer System: An Essential Tool in the Medical Laboratories of Breda," *Medinfo 74*, *op. cit.*

Hennes, James D., et al., *Backgrounds for a Missouri Health Data System*, Columbia, Missouri, Section of Health Care Studies, Department of Community Health and Medical Practice, School of Medicine, University of Missouri, June 30, 1970.

* Henney, C.R.; Brodlie, P.; and Crooks, J.; "The Administration of Drugs in Hospital- How a Computer Can Be Used to Improve the Quality of Patient Care," *Medinfo 74*.

Herner and Company, The Use of Computers in Hospitals, National Center for Health Research and Development, Health Services and Mental Health Administration, Public Health Service, U.S. Department of Health, Education and Welfare, November 1970.

Hershey, John C. and Moore, John R., Jr., "The Use of an Information System for Community Health Services Planning and Management," Medical Care, February 1975, p. 114.

Hickey, William J., "Computer Technology Increased Impact on Medical Record Science," Medical Record News, Vol. 39, October 1968, p. 26.

Hicks, Nancy, "Computer, A Tool in Mental Health," New York Times, May 3, 1970, p.36.

Hicks, Nancy, "Computers Help Hospitals in City To Cut Their Costs," New York Times, February 11, 1971, p. 43.

* Hill, R.D.; Sauter, K.; and Reichertz, P.L.; "The Data Bank Concept of the Medical System Hannover and the Analysis of Patient Data," Medinfo 74, op. cit.

Holloway, Don C., Ph.D.; Wiczai, L. James, M.P.H.; and Carlson, Edgar T., M.P.H.; "Evaluating an Information System for Medical Care Evaluation Studies," Medical Care, April 1975, p. 329.

Holmes, Edith, "'Patient Power' Increases with Diagnostic Systems," Computerworld, November 20, 1974, p. 10.

Honigfeld, Gilbert; Pulier, Myron; Laska, Eugene M.; Kaufl, Robert and Ziek, Peter; "An Approach to Problem-Oriented Psychiatric Records," in Jeffrey L. Crawford et al., Progress in Mental Health Information Systems: Computer Applications.

Hopkins, Carl E., Editor, Methodology of Identifying Measuring and Evaluating Outcomes of Health Service Programs, Systems and Subsystems, California Center for Health Service Research, University of California, Los Angeles, Washington, D.C., U.S. Government Printing Office, 1970.

* Hospital Financial Management Association, The State of Information Processing in the Health Care Industry, August 1970.

"Hospital Pioneers Computerized Preventive Medicine," Government Data Systems, July/August 1975, p. 20.

"Hospital Reporting System Uses NCR 399," Computerworld, October 1, 1975, p. 31.

"Hospital's Budget $1,500/Month Less After CPU Switch," Computerworld, December 10, 1975, p. 37.

"Hospitals Go On-Line with NCR 'Medics,'" Computerworld, October 23, 1974, p. 16.

IBM Application Briefs:

"Data Processing at Prince William Hospital, Manassas, Virginia," GK20-0680-1, March 1974.

"Data Processing in Mental Hospitals with System/13-State of Michigan," GK20-0731-0, January 1974.

"Laboratory Information Processing-Lester E. Cox Medical Center," GK20-0649-0, April 1973.

"Nursing Station Order Entry and Other Online System/370 Applications--Baptist Medical Center," GK20-0717-0, November 1973.

"Human Services Delivery System in Chattanooga," GK20-0655-0, May 1974.

"The Multi-State Information System for Psychiatric Patients," GK20-0607-0.

"Data Processing in the Missouri Divisions of Mental Health," GK20-0659-0, August 1973.

"Online Patient Monitoring at Pacific Medical Center," GK20-0652-0, March 1973.

"Outpatient Care--Cuyahoga County Hospital System," GK20-0737-0, December 1973.

"Patient Administration, Transfer and Discharge with the System/370--Baptist Memorial Hospital," GK20-0630-0, May 1973.

"SLIS at Saint Luke's Hospital Using the IBM System/360," GK20-0637 [illegible], January 1973.

"System/3 Applications at the Sonora Community Hospital and Clinic," GK20-0584-0, September 1972.

"System/3 at Highland Park Hospital," GK20-0642-0, June 1973.

"System/3--Deaconess Hospital," GK20-0111-0, October 1972.

"System/3 in a Specialty Group Practice: Radiology Associates Incorporated," GK20-0615-0, October 1972.

"IBM System for Computerizing Medical Examinations (CME)," GK20-0513-0, July 1971.

"The Department of Institutions, Social and Rehabilitative Services' Information System," GK20-0755-0, January 1975.

"Information Systems Technology in State Government," Report of the National Association for State Information Systems, 1974-75.

* Innes, G. and Weir, R.D., "Patient Identification on a Regional Basis," in McLachlan and Shegog, *Computers in the Service of Medicine, Volume I*.

"Introduction to Computerized Information Processing," *Medical Record News*, August 1973, p. 30.

James, Paul C. and O'Leary, James A., "Automated Medical Records," *Southern Hospitals*, Vol. 38, November 1970, p. 32.

Jenkin, Michael A., M.D., *Clinical Medicine and the Computer*, Proceedings of the Fourth Annual Conference of the Society for Computerized Medicine, New Orleans, Louisiana, November 7-10, 1974.

* Justice, N.; Barnett, G.O.; Lurie, R. and Cass, W.; "Development and Implementation of a Medical/Management Information System at the Harvard Community Health Plan," Proceedings of the 1974 National Computer Conference and Exposition, Chicago, May 6-10, 1974, AFIPS Press, Vol. 43, p. 159.

Kaplan, Jeffrey M. and Smith, William G., "An Evaluation Program for a Regional Mental Health Center," in Jeffrey L. Crawford et al., *Progress in Mental Health Information Systems: Computer Applications*.

* Kauzlarich, C. Vance and Ramm, Dietolf, "Introduction to Data Processing Systems," in Jeffrey L. Crawford et al., *Progress in Mental Health Information Systems: Computer Applications*.

Kelley, Verne R. and Weston, Hanna B., "Computers, Costs, and Civil Liberties," *Social Work*, January 1975, p. 15.

* Kennedy, F.; Cox, A.G.; Glen, A.I.M.; Roy, A.D.; and Sundt, C.E.; "A Computer-Based System for Handling Clinical Data," in McLachlan and Shegog, *Computers in the Service of Medicine, Volume I*.

Kiely, Joseph M., et al., "A Computer-Based Medical Record," *Journal of the American Medical Association*, August 1, 1968, p. 571.

* Klarman, Herbert E., "Application of Cost-Benefit Analysis to Health Systems Technology," *Technology and Health Care Systems in the 1980's, op. cit.*

Klein, Marjorie H., Ph.D., and Greist, John H., M.D., "Computers and Psychiatry," *Archives of General Psychiatry*, July 1975, p. 837.

* Knight, G.J.; Forrer, J.; Wigley, D.; and DeMeyer, T.C.H.; "The Computerized Medical Information System at the Red Cross War Memorial Hospital for Children," *Medinfo 74*, *op. cit.*

Knox, E.G., "Introducing a Computer to a Hospital," in McLachlan and Shegog, *Computers in the Service of Medicine, Volume I*.

Koza, Russell C., Editor, *Health Information Systems Evaluation*, Boulder, Colorado, Colorado Associated University Press, 1974.

Krauss, Marc, et al., "The Use of Data Mechanization and Computers in Clinical Medicine," *Annals of the New York Academy of Sciences*, Vol. 161, September 30, 1969, p. 371.

Kurke, Lewis and Van Houdnos, Harry, "Staff Activity Reporting: From the Bottom-Up," in Jeffrey L. Crawford et al., *Progress in Mental Health Information Systems: Computer Applications*.

* Laska, Eugene M., "The Multi-State Information System," in Jeffrey L. Crawford et al., *Progress in Mental Health Information Systems: Computer Applications*.

* Laska, Eugene M. and Bank, Rheta, *Safeguarding Psychiatric Privacy*, New York, John Wiley & Sons, 1975.

Lawrie, T.D.V. and Macfarlane, P.W., "Towards Automated Electrocardiogram Interpretation," in McLachlan and Shegog, *Computers in the Service of Medicine, Volume I*.

Leighton, R.E., "Use of an Invoice Processing System for Health Data Acquisition," *Medinfo 74*, *op. cit.*

Leslie, Eugene V., "The Medical Staff and the Computerized Medical Record," Right of Privacy and Medical Computing, Conference on the Use of Computers in Medicine, Buffalo, October 2-5, 1969.

Levy, Richard P. and Cammarn, Maxine R., "Information Systems Applications in Medicine," in Cuadra, Carlos A., Editor, Annual Review of Information Science and Technology, Volume 3, Chicago, Encyclopedia Britannica, 1968, p. 397.

Levis, Charles E., M.D. and Deigh, Rosalyn Ann, M.P.H., "An Annotated Inventory of Innovative Changes in Health Care in the United States, 1971-1973," for Project SIC, National Center for Health Services, Research and Development, University of California School of Public Health, Los Angeles, 1973.

* Lindberg, Donald A.B., "A Statewide Medical Information System," Computers and Biomedical Research, Vol. 3, October 1970, p. 453.

Lindberg, Donald A.B., "General Comments," in Jeffrey L. Crawford et al., Progress in Mental Health Information Systems: Computer Applications.

* Lindberg, D., "Medical Education with Hospital Computer Systems," in Morris F. Collen, Hospital Computer Systems.

Lodwick, G., "Information Management in Radiology," in Morris F. Collen, Hospital Computer Systems.

Lubin, Jerome W., et al., Editors, Statistics for Comprehensive Health Planning, Washington, D.C., U.S. Department of Health, Education and Welfare, 1972.

* Ludwig, Herbert, Computer Applications and Techniques in Clinical Medicine, New York, John Wiley & Sons, 1974.

Lunde, Anders S., Ph.D., "The Birth Number Concept and Record Linkage," American Journal of Public Health, November 1975, p. 1165.

Lundell, E. Drake, Jr., "Medical DP Seen Trailing Behind Other Applications," Computerworld, May 15, 1974, p. 27.

Lynch, Martha A., "A Grand Plan for Linkage of Patient Data for a State Mental Health System," Medical Record News, August 1972, p. 65.

McFadden, Robert D., "City-State Pact Set on Computers," New York Times, November 4, 1973, p. 31.

McDonald, Clement; Bhargava, Bharat; and Jervis, David; "A Clinical Information System (CIS) for Ambulatory Care," Proceedings of the 1975 National Computer Conference, p. 749.

McFarlane, A.H., and Norman, G.R., "A Medical Care Information System: Evaluation of Changing Patterns of Primary Care," Medical Care, Vol. 10, 1972, p. 481.

* McLachlan, Gordon and Shegog, Richard A., Editors, Computers in the Service of Medicine, Volume I, London, Oxford University Press, 1968.

McFarlane, A.H. and O'Connell, Brian P., "Morbidity in Family Practice," Canadian Medical Association Journal, Vol. 101,September 6, 1969, p. 259.

McLean, E.R., A Computer-Based Medical History System: Factors Affecting Its Acceptance and Use by Physicians, unpublished Ph.D. Dissertation, Sloan School of Management, Massachusetts Institute of Technology, 1970.

McLean, E.R. and Foote, S., "The Collection and Processing of Medical History Data: A Bibliography of Manual, Automated and Computer-Based Techniques," Information Systems Working Paper 4-75, Graduate School of Management, University of California, Los Angeles, August 1974.

McLean, Ephraim R., "A Comparative Evaluation of Automated Medical History Systems," Proceedings of the 1975 National Computer Conference, p. 733.

McNerney, Walter J., "The Role of Technology in the Development of Health Institutional Goals and Programs," Technology and Health Care Systems in the 1980's, op.cit.

"Medical Histories - 2001?" Hospitals, Vol. 45, February 16, 1971, p. 71.

"Medical Records That Fit a Wallet," Business Week, June 23, 1973, p. 45.

"Medical Word Processing Eliminates Staff Paperwork," Infosystems, July 1973, p. 30.

Merritt, Michael, "One Third of Hospitals Reported Dissatisfied with Vendor Support," Computerworld, November 4, 1970, p. 1.

Mitchell, J.H., "Information Flow in Hospitals," Computers in Medicine, Proceedings of the Second Symposium, Rose, J., Editor, Henry King Ltd., Dorchester, Dorset,1972.

"Mobile Testing Service Keeps Hospitals' Costs Down," Computerworld, January 26, 1976, p. S/10.

Morgan, Donald W. and Crawford, Jeffrey L., "Some Issues in Computer Applications," in Jeffrey L. Crawford et al., Progress in Mental Health Information Systems: Computer Applications.

* Morgan, Donald W. and Frenkl, Sinai I., "Computer Support in Military Psychiatry," in Jeffrey L. Crawford et al., Progress in Mental Health Information Systems: Computer Applications.

Morrill, E. Elbridge; Oser, James L.; and Kusnetz, Howard L.; "Occupational Health Information Systems--Their Concepts and Functions," American Journal of Public Health, Vol. 61, 1971, p. 2469.

Mosher, William E.; Ibrahim, Michael A.; and Van Wie, William; "Coordinated Home Care Information System," Conference on the Use of Computers in Clinical Medicine, Buffalo, October 2-5, 1969.

Mount, Sally A., "Medical Records," Hospitals, Vol. 39, April 1, 1965, p. 125.

Murnaghan, Jane H. and White, Kerr L., Editors, Hospital Discharge Data, Report of the Conference on Hospital Discharge Abstract Systems, Warrenton, Virginia, June 18-20, 1969, Supplement to Medical Care, Vol. 8, 1970.

"NCR Has Small Hospital Turnkey System," Computerworld, November 19, 1975, p. 41.

"National Insurance To Be Supreme 'Test' of DP Privacy Issue," Computerworld, November 20, 1974, p. 11.

Newell, J.A. and Parr, R.F., "Radiotherapy Treatment Planning," in McLachlan and Shegog, Computers in the Service of Medicine, Volume I.

* Nitzberg, D.M., "Basic Neighborhood Health Center Data System," American Journal of Public Health, Vol. 61, October 1971, p. 2065.

Noble, John H., Jr., "Designing Information Systems for Comprehensive Health Planning," Inquiry, Vol. 7, December 1970, p. 34.

Noble, John H., Jr., "In the Health and Welfare Field: The Good and the Bad," Rehabilitation Record, Vol. 13, March-April 1972, p. 14.

Noble, John H., Jr., and Wechsler, Henry, "Obstacles to Establishing Communitywide Information Systems in Health and Welfare," Welfare in Review, November-December 1970, p. 18.

Norwood, D., "Introduction of a User-Oriented THIS into a Community Hospital Setting-Introduction and System Description," Medinfo 74, op. cit.

Ockenden, J.M. and Bodenham, K.E., Focus on Medical Computer Development, published for Nuffield Provincial Hospitals Trust by Oxford University Press, 1970.

O'Connell, B.P. and McFarlane, A.H., A Medical Care Information System: An Approach to the Computerization of Ambulatory Patient Records, August 19, 1969.

O'Kane, K.C. and Hildebrandt, R.J., "An Integrated Health Care Information Processing and Retrieval System," Proceedings of the 1974 National Computer Conference and Exposition, Chicago, May 6-10, AFIPS Press, Vol. 43, p. 93.

Okubo, Ruby, "Record Linkage in Two LA County Hospitals," Medical Record News, August 1972, p. 42.

Opp, Marcia, "The Confidentiality Dilemma," Modern Healthcare, May 1975, p. 49.

Oviatt, Thelma S., "The Kaiser-Permanente System," Medical Record News, February 1972, p. 28.

* Palos, Oscar M., Computer Applications in U.S. Health Care and Insurance, Prepared for the Organization for Economic Cooperation and Development, Paris, France, Stanford Research Institute, December 1968.

"Paperless Claims Net Gets Data at Source," Computerworld, September 10, 1975, p. 29.

Patrikas, Elaine O., RRA, "Caring for the Family as a Family," Medical Record News, April 1967.

Peck, J.D. and Crowder, F.H., "A Public Health Data System" Proceedings of the 1974 National Computer Conference and Exposition, Chicago, May 6-10, 1974, AFIPS Press, Vol. 43, p. 77.

Pollack, Earl S.,; Windle, Charles D.; and Wurster, Cecil R.; "Psychiatric Information System: An Historical Perspective," in Jeffrey L. Crawford et al., Progress in Mental Health Information Systems: Computer Applications.

Pollack, S. R. and Seligman, F., "The Design of a Computerized Health Information System," Conference on the Use of Computers in Clinical Medicine, Buffalo, October 2-5, 1969.

Porter, Karen W., "Computerized Infection Surveillance," Hospitals, Vol. 48, May 1974, p. 83.

Pratt, Arnold W., and Pacak, Milos, "Identification and Transformation of Terminal Morphemes in Medical English," Paper Delivered at Association for Computational Linguistics, University of Illinois, Urbana, July 1968.

Pratt, Arnold W. and Pacak, Milos G.,"Automated Processing of Medical English," Paper Delivered at International Conference on Computational Linguistics, Stockholm, Sweden, September 1-4, 1969.

Price, Elizabeth, "Medical Records," Hospitals, Vol. 41, April 1, 1967, p. 131.

Priest, Steven L., "Hospital, Supermarket Share Unusual DP Relationship," Computerworld, January 26, 1976, p. 32.

Priest, Steven L., "Hospital To Save $15,000/Year with IV Supply, Billing System," Computerworld, October 1, 1975, p. 26.

"Public Health--Productive Health Care: Machine Preventive Medicine," Government Executive, November 1975, p. 28.

* Rader, Dan W., "The Computerized Information System as Organizational Innovation: A Case Study," in Jeffrey L. Crawford et al., Progress in Mental Health Information Systems: Computer Applications.

Rakel, Robert E.,M.D., "The Problem-Oriented Medical Record (POMR)," American Family Physician, September 1974, p. 100.

* Ramm, Dietolf and Gianturco, Daniel T., "The Coming Generation of Psychiatric Information Systems," in Jeffrey L. Crawford et al., Progress in Mental Health Information Systems: Computer Applications.

Rappoport, Arthur E.; Gennaro, William D.; and Berquist, Robert E.; "An On-line Centralized Computer-Coupled Automated Laboratory Information System Using Touch-Tone Card Dialer Telephone and Audio-Response Technology for Test Order Entry and Result Retrieval," Proceedings of 1975 National Computer Conference, p. 757.

Raymond, Samuel, M.D., Ph.D., "Criteria in the Choice of a Computer System; I. The Computer in Theory," Journal of the American Medical Association, April 29, 1974, p. 591.

Raymond, Samuel, M.D., Ph.D., "Criteria in the Choice of a Computer System; II. The Computer in Practice," Journal of the American Medical Association, May 20, 1974, p. 1015.

* Reichertz, P., "University of Hannover Hospital Computer System (Hannover)," in Morris F. Collen, Hospital Computer Systems.

"Report on a Survey of Managerial Opinion on the Impact of Computers in Record-Keeping," in Alan F. Westin and Michael A. Baker, Databanks in a Free Society, New York, Quadrangle Books, 1972.

Ricci, Michael, "Hard Copy Retrieval Tightens Health Controls - Card Document Storage and Retrieval Proves More Effective than Computers or Microfilm," Government Data Systems, May-June 1974, p. 16.

* Richert, R., "Evaluation of a Hospital Computer System," in Morris F. Collen, Hospital Computer Systems.

Richert, Robert H., "The Evaluation of a Medical Data System,"Medical Information Systems, Proceedings of the Conference on Medical Information Systems, U.S. Department of Health, Education and Welfare, Washington, D.C., U.S. Government Printing Office, 1970.

Riggert, W.A., "DP for Dentists Underdeveloped," Computerworld, September 20, 1972, p. 10.

Robinson, Robert E.III, "Acquisition and Analysis of Narrative Medical Record Data," Computers and Biomedical Research, Vol. 3, October 1970, p. 495.

Robinson, R., "Pathology Subsystem," in Morris F. Collen, Hospital Computer Systems.

Rockart, J.T., et al., "An Automated Medical History System: Experience of the Lahey Clinic Foundation with Computer-Processed Medical Histories," Archives of Internal Medicine, Vol. 132, September 1973, p. 348.

Rockoff, Maxine L., "Health Care Communication Systems," in Computer Communications: Impacts and Implications, First International Conference on Computer Communications, Washington, D.C., October 24-26, 1972, p. 465.

Rosenbaum, C. P., "Computer Simplifies Record-Keeping and Review in Psychiatric Clinic," Hospitals, Vol. 42, April 16, 1968, p. 70.

Runck, Howard W., "Information Systems Need Nurses," Datamation, Vol. 14, September 1968, p. 56.

"Rx for Hospitals," Data Processor, Vol. 12, September 1969, p. 4.

Ryan, G.A. and Monroe, K.E., Computer Assisted Medical Practice: The AMA's Role, Center for Health Services Research and Development, American Medical Association, Chicago, 1971.

Salzman, Roy M., "The Computer Terminal Industry: A Forecast," Datamation, November 1975, p. 46.

Saunders, Michael G., "Medical Sector," Datamation, August 15, 1970, p. 31.

Sauter, K., "The Patient Data Bank in a Medical Information System - Tasks, Requirements, Planning and Design," Methods of Information in Medicine, Vol. 12, April 1973, p. 113.

Schmidt, Edward C., M.D., et al., "Computerized Problem Oriented Medical Record for Ambulatory Practice," Medical Care, April 1974, p. 316.

Schmitz, H. H., "Evaluation of a Modular Hospital Information System," Hospital Progress, Vol. 53, June 1972, p. 70.

Schneider, Judith, "The Nurse in a Computerized Environment," Computerization of Clinical Records, E. R. Gabrieli, Editor, New York, Grune and Stratton, 1970.

Section of General Practice of the Royal Society of Medicine, "Record Linkage in General Practice," Practitioner, Vol. 204, March 1970, p. 441.

Shannon, Roger H.,M.D., "The Second Wave; A Reexamination of Computers in Medicine," Postgraduate Medicine, April 1975, p. 55.

Shepley, D.J., "A Health Information System for Ten Million People," in Medinfo 74, op. cit.

Sheridan, Dan, "Kicking the Addict Registry Habit," The Bergen Record, November 22, 1974, p. C-3.

Silverstein, Martin E., "Computers, Communications and Distributed Health Care Systems," in Computer Communications: Impacts and Implications, First International Conference on Computer Communications, Washington, D.C., October 24-26, 1972,p.463.

Singer, J. Peter, "Computer-Based Hospital Information Systems," Datamation, Vol. 15, May 1969, p. 38.

Slack, Warner V., et al., "A Computer-Based Medical History System, New England Journal of Medicine, Vol. 274, January 27, 1966, p. 194.

Sletten, Ivan W. and Hedlund, James L.,"The Missouri Automated Standard System of Psychiatry: Current Status, Special Problems and Future Plans," in Jeffrey L. Crawford et al., Progress in Mental Health Information Systems: Computer Applications.

Soghikian, K., "Preventive Health Maintenance Clinics,"in Morris F. Collen, Hospital Computer Systems.

* "Special Issue: Automated Multiphasic Health Testing," Hospitals, Vol. 45, March 1, 1971.

"Special Issue: Psychiatry and the Computer," Comprehensive Psychiatry, Vol. 8, December 1967.

Spencer, William A., "Consumer Expectations of Technology," Technology and Health Care Systems in the 1980's, op. cit.

Spitzer, Robert L. and Endicott, Jean, "Computer Diagnosis in Automated Recordkeeping Systems: A Study of Clinical Acceptability," in Jeffrey L. Crawford et al., Progress in Mental Health Information Systems: Computer Applications.

* Stacy, Ralph W. and Waxman, Bruce D., Editors, Computers in Biomedical Research, Volume II, New York, Academic Press, 1965.

Stangle, Bruce E., "An Analysis of Computer Security in an Ambulatory Medical Care Facility," Master's Thesis, Massachusetts Institutue of Technology, 1974.

Stern, R.B.; Knill-Jones, R.P.; and Williams, Roger; "Use of Computer Program for Diagnosing Jaundice in District Hospitals and Specialized Liver Unit," British Medical Journal, June 21, 1975, p. 659.

Straach, H.P. and Griesser, G., "Interaction of a Hospital Information System with a Regional Sickness Fund Information System," Medinfo 74, op. cit.

* Streeter, Donald N., The Scientific Process and the Computer, New York, John Wiley & Sons, 1974.

* Summary Report on Hospital Information Systems, Health Care Technology Program, National Center for Health Services Research and Development, Health Services and Mental Health Administration, Public Health Service, U.S. Department of Health, Education and Welfare, June 1969.

"Survey Prescribes Off-line Data Entry for Medical Insurance Firm," Infosystems, September 1975, p. 68.

"T/S System at Hospital Improves Patient Support," Computerworld, December 10, 1975, p. 42.

Taplin, R. Clinton, "Mental Health Data Bank Spurned," The Bergen Record, March 29, 1973, p. A-14.

Taylor, Thomas, "Computers in Medicine," Science Journal, Vol. 7, October 1970, p.81.

Terdiman, J., "Physiological Monitoring Systems," in Morris F. Collen, Hospital Computer Systems.

Terdiman, J.F.; Van Brunt, E.E.; Davis, Lou S.; and Collen, M.F.; "A Pilot Computer System for Health Care Delivery to a Community," Medinfo 74, op. cit.

Thomas, A.W., "Experience with an On-Line Patient Information System," Medinfo 74, op. cit.

Trainer, Peter E., "Advanced Computer-Based System Screens Medicaid Claims in Albany County, New York," Communication News, January 1974.

Tyler, C.R., "Approaches to Hospital Information Systems," Medinfo 74, op. cit.

U.S. Department of Health, Education and Welfare, Development of the Design of the NCHS Hospital Discharge Survey, Washington, D.C., U.S. Government Printing Office, September 1970.

The Use of Computers in Hospitals, Report of Contract PH110-233, U.S. Department of Health, Education and Welfare, Washington, D.C., U.S. Government Printing Office, 1969.

* The Use of Computers in Medicine: A Bibliography, Defense Documentation Center, Alexandria, Virginia, May 1974.

* Vallbona C. and Spencer, W., "Texas Institute for Research and Rehabilitation Hospital Computer System (Houston)," in Morris F. Collen, Hospital Computer Systems.

Van Brunt, E. and Collen, M., "Nursing Station Subsystem," in Morris F. Collen, Hospital Computer Systems.

* Van Brunt, E.; Davis, L.; and Collen, M.; "Kaiser-Permanente Hospital Computer System," in Morris F. Collen, Hospital Computer Systems.

Vogler, T., "The Sisters of Saint Mary Multi-Hospital Information System," Seminar on Computer Applications in the Field of Medicine, Sperry/Univac International Executive Centre, Rome, April 2-4, 1975.

Wachs, Melvin W., "Planning-Programming-Budgeting and Management Information Systems for Mental Health," American Journal of Public Health, Vol. 59, 1969, p. 261.

Wade, O.L., "The Computer and Drug Prescribing," in McLachlan and Shegog, Computers in the Service of Medicine, Vol. I.

Ward, Patrick, "Microfilmed Billing Records Save $50,000/Year," Computerworld, December 3, 1975/January 5, 1976, p. 30.

* Warner, Homer R., "Problems and Priorities for Health Care Technology," Technology and Health Care Systems in the 1980's, op. cit.

Watson, R.J., "Medical Staff Response to a Medical Information System with Direct Physician-Computer Interface," Medinfo 74, op. cit.

Waxman, Bruce D., "Health Care Delivery--The Impact of Recent Technological Developments," Proceedings of the 1973 National Computer Conference, p. M45.

Weed, Lawrence L., M.D., Your Health Care and How To Manage It, Burlington, Vermont, PROMIS Laboratory, University of Vermont, 1975.

Weinstein, Michael, "Security Plan 12 Years Ahead of Time?" Computerworld, November 15, 1972, p. 23.

Weir, R.D.; Crooks, J.; and Coull, D.C.; "The Development of Drug Monitoring for Side-effects within a Hospital Medical Information System," in McLachlan and Shegog, Computers in the Service of Medicine, Volume I.

* White, D., "Information Processing of Medical Records - State of the Art: April 1970," Methods of Information in Medicine, Vol. 9, July 1970, p. 189.

Whitehead, T.P.; Becker, J.F.; and Peters, M.; "Data Processing in a Clinical Biochemistry Laboratory," Computers in the Service of Medicine, Vol. I., McLachlan and Shegog, Editors.

"Wide Variety of Computer Based Systems Available to Hospitals," Datamation, March 1975, p. 115.

Wiederhold, Gio; Fries, James F., M.D.; and Weyl, Stephen; "Structured Organization of Clinical Data Bases," National Computer Conference, Anaheim, California, May 19-23, 1975.

Williams, D., "The Administrative System," in Morris F. Collen, Hospital Computer Systems.

Williams, Douglas A., "Kaiser-Permanente Information Systems: A Review and Evaluation," in Russell C. Koza, Health Information Systems Evaluation, op. cit.

Williams, George Z., "The Impact of Emerging Technology on Health Evaluation and Maintenance," Technology and Health Care Systems in the 1980's, op. cit.

Williams, G. and Williams, R., "Clinical Laboratory Subsystem," in Morris F. Collen, Hospital Computer Systems.

Wilson, Nancy C., "An Information System for Clinical and Administrative Decision-Making, Research, and Evaluation," in Jeffrey L. Crawford et al., Progress in Mental Health Information Systems: Computer Applications.

Wilson, Vernon E., "Use of Total Population Data System for Development and Evaluation of the Regional Medical Program--Report from Missouri,"American Journal of Public Health, Vol. 58, 1968, p. 1054.

Wiseman, Toni, "Decade of the User Brings End to Closed Environment," Computerworld, October 29, 1975, p. 12.

Wiseman, Toni, "National Bank of Birth Defects To Zero In on Patterns, Causes," Computerworld, June 26, 1974, p. 36.

Yanez, L.M., "Introduction of a User-Oriented THIS into a Community Hospital Setting - Confidentiality and Security," Medinfo 74, op. cit.

Yarnall, S.R. and Wakefield, J.S., Acquisition of the History Database, (2nd ed.), Seattle, Washington, Medical Computer Services Association, 1972.

Young, Elmer D., "Data Bank for Narcotic Addicts," Computers and Automation, October 1970, p. 40.

CITIZEN RIGHTS ISSUES IN HEALTH CARE

"AHA Patients Bill of Rights," Medical Record News, October 1973, p. 81.

* A Guide for Cooperation with Communications Media, Chicago, American Hospital Association, 1974.

Ad hoc Committee on Ethical Standards in Psychological Research, Ethical Principles in the Conduct of Research with Human Participants, Washington, D.C., American Psychological Association, 1973.

"Adoptees Fight Sealed-Record Policies To Learn Background," Freedom of Information Digest, November-December 1975.

*Alfano, Guy E., "Privacy of the Data Generator," Right of Privacy and Medical Computing, Conference on the Use of Computers in Medicine, Buffalo, New York, October 2-5, 1969.

Altman, Lawrence K., "Doctor and Patient: Bill of Rights a Break with Old Paternalism," New York Times, January 10, 1973, p. 24.

Altman, Lawrence K., "Hospital Moved Eagleton Data," New York Times, July 30, 1972, p. 1.

* American Medical Record Association, "Statement on the Preservation of Patient Medical Records in Health Care Institutions," Medical Record World, December 1973, p. 31.

American Psychiatric Association, "Position Statement on Confidentiality and Privilege with Special Reference to Psychiatric Patients," American Journal of Psychiatry, Vol. 124, January 1968, [illegible] 1015.

American Psychiatric Association, "Position Statement on Guidelines for Psychiatrists: Problems in Confidentiality," American Journal of Psychiatry, Vol. 126, April 1970, p. 1543.

* American Psychiatric Association, "Position Paper on the Confidentiality of Medical Research Records," American Journal of Psychiatry, Vol. 130, June 1973, p. 739.

American Psychiatric Association, "Position Statement on the Need for Preserving Confidentiality of Medical Records in Any National Health Care System," American Journal of Psychiatry, Vol. 128, April 1972, p. 1349.

* Annas, George J., "A.H.A. Bill of Rights," Trial, November/December 1973, p. 59.

Annas, George J., "The Hospital: A Human Rights Wasteland," Civil Liberties Review, Fall 1974, p. 9.

Annas, George J., "Law and Psychiatry: When Must the Doctor Warn Others of the Potential Dangerousness of His Patient's Condition?" Medicolegal News, April 1975, p. 1.

* Annas, George J., The Rights of Hospital Patients, Boston, Center for Law and Health Sciences, April 1, 1974.

* Annas, George J. and Healey, Joseph M. Jr., "The Patient Rights Advocate: Redefining the Doctor-Patient Relationship in the Hospital Context," Vanderbilt Law Review, Vol. 27, 1974, p. 243.

Babineau, G. Raymond, "The Contract of Secrecy," Mental Health Digest, Vol. 4, May 1972, p. 20.

* Beard, Margaret C. and Springer, Eric W., "Patient's Health Records Must Be Protected," Nursing Home Administration, Vol. 20, March/April 1966, p. 87.

* Bergen, Richard P., "Keeping the Patient's Secrets," Journal of the American Medical Association, Vol. 195, January 31, 1966, p. 227.

* Bernstein, A. H., "Protecting Psychiatric Records," Hospitals, Vol. 47, October 1, 1973, p. 100.

Bernstein, A. H., "The Quest for Hospital Records," Hospitals, Vol. 45, October 1, 1971, p. 100.

* Biegler, Jerome S., "1971 Amendment of the Illinois Statute on Confidentiality: A New Development in Privilege Law," American Journal of Psychiatry, Vol. 129, September 1972, p. 311.

Bohm, K., "Protection and Confidentiality of Medical Data: Simple Methods for Meeting the Users' Needs," Medinfo 74, op. cit.

Bowden, Lois A., "May a Physician's Office History Be Included in the Patient's Hospital Medical Record?" Hospitals Vol, 47, November 16, 1973, p. 12.

"Bridging the Gap - Psychiatrist Patient Privilege," Medical Insight, August 1972, p. 61.

Britton, Ann H., "Rights to Privacy in Medical Records," The Journal of Legal Medicine, July/August 1975, p. 30.

Brody, Jane E., "Psychiatrist Alarmed by 'Steady Invasion' of Confidential Communications with Patients," New York Times, June 21, 1973, p. 19.

Brown, Rowine Hayes, "Controlling Child Abuse: Reporting Laws," Case and Comment, January-February 1975, p. 10.

Bulger, Roger J., M.D., Editor, Hippocrates Revisited, New York, Medcom Press, 1973.

Bumbalo, Thomas S., "Protection of Medical Personnel in Computerized Data Systems," Right of Privacy and Medical Computing, Conference on the Use of Computers in Medicine, Buffalo, October 2-5, 1969.

"The Campaign To Protect Personal Privacy," Business Week, January 16, 1974, p. 88.

Capell, Martin D., "Research and Privacy," and Strickler, George, "On Research and Privacy," Psychotherapy Bulletin, April 1970, p. 4.

Carroll, James D., "Confidentiality of Social Science Research Sources and Data: The Popkin Case," *PS*, American Political Science Association, Vol. 6, Summer 1973.

* Carroll, John M., *Assuring Information Protection in the Health Sector*, Seminar on Policy Issues in Data Protection - Concepts and Perspectives, Paris, France, June 24-26, 1974.

* Chiles, Robert E., "The Rights of Patients," *The New England Journal of Medicine*, Vol. 277, August 24, 1967, p. 109.

"Clinical Information and Records - Public or Confidential?" *The New England Journal of Medicine*, Vol. 270, June 4, 1964, p. 1240.

Closson, W.G., Jr., et al., "Confidentiality in Psychiatry and Psychotherapy," *California Medicine*, Vol. 113, October 1970, p. 12.

* Cole, Nyla J., "Psychiatrists, Employers and Information Exchange," *Archives of General Psychiatry*, Vol. 25, October 1971, p. 381.

"Computerized Records Are Legal Risk," *Modern Hospital*, Vol. 117, July 1971, p. 45.

"Confidential Information Must Be Protected," *American Medical News*, January 7, 1974, p. 4.

Confidentiality and Third Parties, Report of the Task Force on Confidentiality As It Relates to Third Parties, American Psychiatric Association, Washington, D.C., 1975.

* *Confidentiality: Report of the Conference on Confidentiality of Health Records*, Key Biscayne, Florida, November 6-9, 1974, Washington, D.C., American Psychiatric Association, 1975.

Converse, Mary E., "Privacy of the Hospital Medical Record," *Right of Privacy and Medical Computing*, Conference on the Use of Computers in Medicine, Buffalo, 1969.

* Crystal, Royal A., "Maintenance of Confidentiality and Protection of Privacy in Computer Based Health Data Banks," *Right of Privacy and Medical Computing*, *op. cit.*

Curran, William J., "Policies and Practices Concerning Confidentiality in College Mental Health Services in the United States and Canada," *American Journal of Psychiatry*, Vol. 125, May 1969, p. 1520.

* Curran, William J.; Stearns, Barbara; and Kaplan, Honora; "Privacy, Confidentiality and Other Legal Considerations in the Establishment of a Centralized Health-Data System," *The New England Journal of Medicine*, Vol. 281, July 31, 1969, p. 241.

* Curran, William J; Laska, Eugene M.; Kaplan, Honora and Bank, Rheta; "Protection of Privacy and Confidentiality," *Science*, Vol. 182, November 23, 1973, p. 797.

* Daechsel, Werner P.O., "Medical Computing and Privacy Issues in Canada," *Right of Privacy and Medical Computing*, *op. cit.*

"Data Taps Threaten Patient-MD Bond, "*Medical World News*, Vol. 14, June 1, 1973, p.17.

"The Dearth and Death of Privacy," *Journal of the Medical Society of New Jersey*, Vol. 67, May 1970, p. 205.

* Dewitt, Clinton, *Privileged Communications Between Physician and Patient*, Springfield, Illinois, Charles C. Thomas, 1958.

Dinklo, J.A., "Confidentiality of Medical Data in the Usage of Data Banks," *Medinfo 74*, *op. cit.*

"Disclosure of Medical Record Information," *Hospitals*, Vol. 39, October 1, 1965, p. 103.

Dr. Martin Luther King, Jr. Health Center, *Your Rights As A Patient*, Bronx, New York, 1974.

Dubey, Joseph, M.D., "Confidentiality as a Requirement of the Therapist: Technical Necessities for Absolute Privilege in Psychotherapy," *American Journal of Psychiatry*, October 1974, p. 1093.

* Durham, Samuel C., "Right to Privacy - Confidentiality of Mental Illness Files," *Gonzaga Law Review*, Vol. 7, Fall 1971, p. 106.

* English, Charles O., *Report on Examination of the Medical Information Bureau as of December 31, 1971*, Albany, State of New York Insurance Department, May 15, 1973.

* Ennis, Bruce and Siegel, Loren, *The Rights of Mental Patients: The Basic ACLU Guide to a Mental Patient's Rights*, New York, Discus Books, 1973.

* Entmacher, Paul S. and Gutman, Jeremiah S., "Computerized Insurance Records: To Whom Should They Be Released?" *Hastings Center Report*, November 1973, p. 8.

Ericsson, Ulla; Schneider, W. and Vogel, K.: "The Problem of Privacy in a Computer Based Integrated Health Care Information System," Medinfo 74, op. cit.

Errara, Paul, "Common-sense Approaches to Confidentiality," Hospital and Community Psychiatry, Vol. 19, November 1968, p. 347.

Etziony, M.B., The Physician's Creed, Springfield,Illinois, Charles C. Thomas, 1973.

Fairhall, John, "Privacy, The Silent Invasion: You Gave Away Your Privacy," Albany Times-Union, December 8, 1975, p. 1.

Fanning, John P.; Martin, David B.H.; and Bennett, Susan J., "Fair Information Practice for Health and Medical Records," Conference on the Confidentiality of Health Records, Key Biscayne, Florida, November 6-9, 1974.

* Federal Data Banks and Constitutional Rights: A Study of Data Systems on Individuals Maintained by Agencies of the U.S. Government, Subcommittee on Constitutional Rights, Committee on the Judiciary, U.S. Senate, Volumes 1-4, and Staff Report, Washington, D. C.,U.S. Goverrment Printing Office, 1974.

* Federal Information Systems and Plans - Implications and Issues, Hearings Before a Subcommittee of the Committee on Government Operations, House of Representatives, Ninety-third Congress, Second Session, Washington, D.C., U.S. Government Printing Office, 1974.

Fischer, T.H. and Helmbock, J.M., "Data Privacy and Data Security in Kiel KIS," Medinfo 74, op. cit.

Fosburgh, Lacey, "Methadone Clinic Head Sentenced for Contempt," New York Times, July 26, 1972, p. 62M.

* Freed, Roy N., "A Legal Structure for a National Medical Data Center," Boston University Law Review, Vol. 49, 1969, p. 79.

"The Freedom of Medical Information," Journal of the American Medical Association, July 14, 1975, p. 145.

Furner, Joanne F. and Thomason, J. William, "Physician-Patient Confidences:Legal Effects of Computerization of Records," The Alabama Lawyer, Vol. 31, April 1970, p. 193.

* Gabrieli, E.R., Editor, Journal of Clinical Computing, Vol. 4, Transactions of the 6th Buffalo Conference on Ethical Data Centers, Buffalo, New York 1974.

* Ginsberg, Harvey N., Report on Examination of the Medical Information Bureau as of December 31, 1965, Albany, State of New York Insurance Department, March 15, 1967.

"Give the Patient His Medical Record, Swedish Doctor Urges," Modern Hospital, Vol. 120, May 1973, p. 44.

Goldie, Ray R., "The Requirements of Informed Consent," Hospitals, Vol. 46, May 16, 1972, p. 58.

Golodetz, Arnold, M.D.; Ruess, Johanna, M.D.; and Milhous, Raymond L.; "The Right To Know: Giving the Patient His Medical Record," paper presented at 1974 meeting of American Congress of Rehabilitation in Medicine and the American Academy of Physical Medicine.

* Grann, Richard, "Considerations of Privacy in the World of Computer-Based Information Systems," Prepared for Presentation at the Annual Health Conference of the Public Health Conference of the New York State Public Health Association and the New York State Association for Mental Health, Rochester, New York, June 10,1968.

Gray, Bradford H., Human Subjects in Medical Experimentation, New York, John Wiley & Sons, 1975.

Gribbin, August, "Insurance Firms Maintain Secret Data Repository," National Observer, November 3, 1969.

* Grossman, Maurice, "Insurance Reports as a Threat to Confidentiality," American Journal of Psychiatry, Vol. 128,July 1971, p. 64.

Grossman, Maurice, M.D., "The Psychiatrist and the Subpoena," The Bulletin of the American Academy of Psychiatry and the Law, December 1973, p. 245.

Group for the Advancement of Psychiatry, Confidentiality and Privileged Communication in the Practice of Psychiatry, Report No. 45, New York, June 1960.

"Guidelines Concerning the Ethical Storage and Retrieval of Privileged Medical Information in Computers," Pennsylvania Medicine, Vol. 73, December 1973.

* Guidelines for Maintaining Confidentiality of Patient Records, Springfield,Illinois, Illinois Department of Mental Health, 1974.

Halleck, Seymour L., "Legal and Ethical Aspects of Behavior Control," The American Journal of Psychiatry, Vol. 131, April 1974, p. 381.

Hassard, Howard,"Privileged Communications: Physician-Patient Confidences in California," California Medicine, Vol. 90, 1959, p. 411.

Hawkland, William D., "Legislative Approach to Control Computer-Stored Health Data," Right of Privacy and Medical Computing, op. cit.

Hayt, Emanuel, "Court in Error in Demanding Entire Hospital Record Be Admitted," Hospital Management, Vol. 106, July 1968, p. 18.

"Health and Privacy: Patient Records, A Report of Current Practices with Recommendations for Changes," Massachusetts Governor's Commission on Privacy and Personal Data, November 1974.

Herr, Conrad E. A., "The Hospital Information System, A Worry Piece," Medical Record News, Vol. 45, June 1974, p. 6.

Hall, George E., "Privileged Communications Statutes," Journal of the American Medical Association, Vol. 207, February 17, 1969, p. 1415.

* Hershey, N., "When Is a Communication Privileged?" American Journal of Nursing, Vol. 70, January 1970, p. 112.

Hofmann, Adele D., M.D., "Confidentiality and the Health Care Records of Children and Minor Youth," Conference on the Confidentiality of Health Records, Key Biscayne, Florida, November 6-9, 1974.

Holder, Angela Roddey, "Disclosure of Confidential Information," Journal of the American Medical Association, Vol. 216, April 12, 1971, p. 385.

Holmes, William, "Privacy Techniques for Computerized Medical Data Systems," Right of Privacy and Medical Computing, op. cit.

Horty, John F., "Cases Clarify Staff Privileges, Guardians' Rights, Negligence," Modern Hospital, Vol. 116, April 1971, p. 88.

Horty, John F., "Court's Need Can Impose Limits on Physician-Patient Privilege," Modern Hospital, Vol. 113, August, 1969, p. 54.

Horty, John F., "Medical Records Aren't Fishing Grounds: Court," Modern Hospital, Vol. 116, March 1971, p. 68.

Horty, John F., "Only Patient Can Permit Examination of His Record," Modern Hospital, Vol. 117, September 1971, p. 71.

Horty, John F., "Plaintiff Wins Right To Examine Hospital's Internal Working Papers," Modern Hospital, Vol. 115, August,1970, p. 48.

Horty, John F., "Recent Court Cases Deal with Rules, Standards and Information Duties," Modern Hospital, Vol. 115, July 1970, p. 62.

"How To Reassure Patients' Anxiety: Show Them Their Hospital Records," Medical World News, January 13, 1975, p. 48.

* Hussey, Hugh H., "Privacy of Patient's Records," Journal of the American Medical Association, Vol. 226, November 19, 1973, p. 995.

* Illinois Medical Record Association, Handbook on Release of Information and Reporting from Medical Records, Berwyn,Illinois, Press of Physicians' Record Company,1970.

Indian Health Care, Hearings before the Permanent Subcommittee on Investigations of the Committee on Government Operations, U.S. Senate, 93rd Congress, Second Session, Washington, D.C., U.S. Government Printing Office, 1974.

"Insurance Data Bank Attacked as Abuse of Confidentiality," Hospital Practice, Vol. 7, August 1972, p. 47.

"Judge Stays a Law on Computerizing Prescribed Drugs," New York Times, March 31, 1973, p. 70.

* Kane, Stanley D., "Recent Judicial Trends in Medical Privilege," Modern Medicine, May 1, 1972, p. 106.

King, James P., "Handling Personal, Confidential Information," Virginia Medical Monthly, Vol. 94, May 1967, p. 279.

Knoll, David D., "The Physician-Patient Privilege, Article 31, and the Military Doctor," Military Medicine, Vol. 136, July 1971, p. 640.

Land, Thomas, "An Addict's Right to Privacy," Data Systems, June 1974, p. 28.

"Lawyer Inspection of Records Upheld," New York Times, March 24, 1973, p. 37.

• Olafson, Freya; Ferguson, Allen Jr.; and Parker, Alberta W.; Confidentiality: A Guide for Mental Health Centers, San Francisco, Pisani Printing Company, 1971.

Opp, Marcia, "The Confidentiality Dilemma," Modern Health, May 1975, p. 49.

Parker, Leo T., "Right to Hospital Records," Hospital Topics, Vol. 47, January 1969, p. 3[illegible].

"Patient's Chart: An Open Book?" Hospitals, Vol. 40, January 1, 1966, p. 90.

Perles, Julia, "Confidentiality, Privilege and Responsibility: Legal and Ethical Problems," New York State Journal of Medicine, Vol. 65, October 15, 1965.

Peterson, H., "A Password Oriented Privacy System for Stockholm County," Medinfo 74, op. cit.

"Physician's Reporting of Narcotic Addicts As Required by Statute," New Physician, Vol. 21, March 1972, p. 172.

Pierce, Chester M., "Who's Giving Away the Patient's Secrets?" Medical Economics, Vol. 46, April 28, 1969, p. 227.

Plank, Robert, "Our Underprivileged Communications," Social Casework, Vol. 46, July 1965, p. 430.

Porterfield, John D. III, "How Should Records of Psychiatric Patients Be Kept and Filed?" Hospitals, Vol. 39, August 16, 1965.

Prism, Special Issue on Privacy, June 1974.

Privacy, the Census and Federal Questionnaires, Hearings before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, 91st Congress, First Session, on S. 1791, Washington, D.C., U.S. Government Printing Office, 1970.

"Protecting Individual Privacy in Evaluation Research," Washington, D.C., National Academy of Sciences, 1975.

Ramsey, Paul, The Patient as a Person, New Haven, Yale University Press, 1970.

Reed, I.S., "Information Theory and Privacy in Data Banks," Proceedings of the 1973 National Computer Conference and Exposition, New York, June 4-8, 1973, AFIPS Press, Vol. 42, p. 581.

Regan, William A., "Hospital's Duty To Disclose Medical Record to Next of Kin: Washington, D.C., "Hospital Progress, Vol. 49, May 1968, p. 6.

Reid, Michael H., "Fishing Through Patient Records," Medical Care, Vol. 10, November-December 1972, p. 488.

Report of the American Civil Liberties Union Privacy Committee on Medical Records, Alan F. Westin, Chairperson, New York, American Civil Liberties Union, 1973.

• Right of Privacy and Medical Computing, Conference on the Use of Computers in Clinical Medicine, Buffalo, New York, October 2-5, 1969.

Ritter, Robert C., "Patient-Physician Privilege in the Discovery Process," South Dakota Law Review, Vol. 17, Winter 1972, p. 188.

• Robitscher, Jonas B., "Doctors' Privileged Communications, Public Life and History's Rights," Cleveland-Marshall Law Review, Vol. 17, May 1968, p. 199.

Rosenberg, Arthur Harris, "Compulsory Disclosure Statutes," New England Journal of Medicine, Vol. 280, June 5, 1969, p. 1287.

Ruben, Harvey L., "Confidentiality and Privileged Communications: The Plight of the Military Physician," Military Medicine, Vol. 138, April 1973, p. 211.

Rumsey, J.M., "[illegible]al Records Must Remain Confidential," American Medical News, Vol. 16, November [illegible] 1973, p. 20.

Sacks, Herbert S., [illegible]., "Title XX: A Major Threat to Privacy and a Setback for Informal Consent," Connecticut Medicine, December 1975.

Schoolar, Joseph C., Ph.D., M.D., and Gaitz, Charles M., M.D., Research and the Psychiatric Patient, New York, Brunner/Mazel, 1975.

Shah, Saleem, A., "Privileged Communications, Confidentiality and Privacy," Professional Psychology, Fall, 1969, p. 56.

• Shenkin, Budd D. and Warner, David C., "Giving the Patient His Medical Record: A Proposal To Improve the System," New England Journal of Medicine, Vol. 289, September 27, 1973, p. 688.

• Sigerist, Henry E., Medicine and Human Welfare, New Haven, Yale University Press, 1941.

* "Legal Aspects of Computerized Information Systems," The Honeywell Computer Journal, Vol. 7, 1973.

Letourneau, Charles U., "Erosion of the Professional Secret," Hospital Management, Vol. 99, January 1965, p. 53.

Lewis, Melvin, "Confidentiality in the Community Mental Health Center," American Journal of Orthopsychiatry, Vol.27, October 1967, p. 946.

"Life Firms' Confidentiality Questioned," The Journal of Commerce, October 21, 1974, p. 9.

* Luger, Rosalind Massow, "The Ordeals of Confidentiality," Physician's World, June 1974, p. 23.

Lyons, Richard D., "Insurance Data Called Faulty," New York Times, October 4, 1973, p. 22.

MacMahon and Taeuber, "Privacy and Confidentiality in Collecting and Using Health Statistics," Report of the Twentieth Anniversary Conference of the U.S. National Committee on Vital and Health Statistics, Vital and Health Statistics, September 1970, p. 3.

* McCaffrey, Sr.Mary P., "Implications of Confidentiality in the Doctor-Patient Relationship," Hospital Progress, Vol. 54, December 1973, p. 63.

McLaughlin, Marsha Morrow and Vaupel, Suzanne, "Constitutional Right of Privacy and Investigaive Consumer Reports: Little Brother Is Watching You," Hastings Constitutional Law Quarterly, Summer 1975, p. 773.

McNamara, James, "Legal Aspects of Computerized Medical Records," Journal of the American Medical Association, Vol. 191, March 15, 1965, p. 951.

McNamara, Robert M., Jr. and Stan, Joyce R., "Confidentiality of Narcotic Addict Treatment Records: A Legal and Statistical Analysis," Columbia Law Review, Vol. 73, 1973, p. 1579.

McNinch, Joseph H., "Release of V.A. Hospital Records to Private Physicians," Journal of the American Medical Association, Vol. 191, March 15, 1965, p. 951.

"Medical Jurisprudence - Privileged Communications Between Physician and Patient - State Regulation and Right to Privacy," Tennessee Law Review, Vol. 39, Spring 1972, p. 515.

Medical Privacy and Computer Technology, Transactions of the Joint Task Group of the Medical Society of the County of Erie, Volume I, Buffalo, New York, Reproduced by the Journal of Clinical Computing, Inc., 1974.

Manninger, W.W. and English, Joseph T., "Confidentiality and the Request for Psychiatric Information for Nontherapeutic Purposes," American Journal of Psychiatry, Vol. 122, December 1965, p. 638.

Mental Health Services and the General Hospital: A Guide to the Implementation of Mental Health Service Plans, Chicago, American Hospital Association, 1970.

"Michigan Court Dismisses Medical Record Suit," Hospitals, Vol. 46, January 1, 1972, p. 107.

Modlin, Herbert C., "How Private Is Privacy," Psychiatric Digest, February 1969, p. 13.

Mondello, Anthony L., "Protection of Privacy Rights in Computerized Data Systems," Right of Privacy and Medical Computing, op. cit.

Morse, Howard Newcomb, "Physician's Liability for Improper Disclosure," Journal of the American Medical Association, Vol. 198, November 14, 1966, p. 331.

"Must a Wisconsin Physician Report?" Wisconsin Medical Journal, Vol. 72,January 1973, p. 43.

Neier, Aryeh, Dossier: The Secret Files They Keep on You, New York, Stein and Day, 1975.

Nelson, Harry, "Threat to Patients' Privacy Right Seen," Los Angeles Times, December 3, 1973, p. 1.

* Noble, John H. Jr., "Protecting the Public's Privacy in Computerized Health and Welfare Systems," Social Work, Vol. 16, January 1971, p. 35.

* Nunn, James R., "Privacy of the Patient: Medical Aspects of Privileged Communications," Right of Privacy in Medical Computing, op. cit.

Simmons, Dale D., "Client Attitudes Toward Release of Confidential Information Without Consent," Journal of Clinical Psychology, Vol. 24, July 1968, p. 364.

* Slawson, P. F., "Patient-Litigant Exception: A Hazard to Psychotherapy," Archives of General Psychiatry, Vol. 21, September 1969, p. 347.

* Slovenko, Ralph, "Psychotherapist-Patient Testimonial Privilege: A Picture of Misguided Hope," Catholic University Law Review, Vol. 23, Summer 1974, p. 649.

Solomon, Philip; Kleeman, Susan T. and Curran, William J.; "Confidentiality in Psychiatric Screening for Security Clearance," American Journal of Psychiatry, Vol. 127, May 1971, p. 1566.

Special Action Office for Drug Abuse Prevention, "Confidentiality of Drug Abuse Patient Records," Federal Register, Vol. 37, November 17, 1972, p. 24636.

Spingarn, Natalie Davis, "Eavesdroppers Behind the Doctor's Door," Washington Post, June 1, 1975, p. C1.

Springer, E.W., "Physician-Patient Privilege: Two Rulings For, One Against," Hospital Topics, Vol. 51, September 1973, p. 37.

Springer, Eric W., "Are Psychiatrist-Patient Communications Protected by the Constitution?" Medical Record News, Vol. 42, August 1971, p. 61.

* Springer, Eric W., Automated Medical Records and the Law, Pittsburgh, Aspen Systems Corporation, 1971.

* Statement Against Use of Social Security Numbers for Hospital Medical Records, Chicago, American Hospital Association, 1974.

Statement of John Smiley, Right of Privacy and Medical Computing, op. cit.

"Statement of Principles Concerning the Confidentiality of Medical Information," Health Insurance Association of America, October 24, 1974.

* Statement on a Patient's Bill of Rights, Chicago, American Hospital Association, 1972.

* Statement on Health Data Systems, Chicago, American Hospital Association, 1973.

* Statement on Preservation of Patient Medical Records in Health Care Institutions, Chicago, American Hospital Association, 1974.

* Statement on the Right of the Patient To Refuse Treatment, Chicago, American Hospital Association, 1974.

Steeves, Robert F., "A Question of Privilege: Releasing Prescription Record Information," Journal of the American Pharmaceutical Association, Vol. NS5, August 1965, p. 448.

Stetson, E. Blythe, "The Role of Law in Medical Progress," Law and Contemporary Problems, Vol. 32, Autumn 1967, p. 563.

* Subcommittee on Constitutional Rights of the Committee on the Judiciary, U.S. Senate, Federal Data Banks and Constitutional Rights, Volumes 1-6, Washington, D.C., U.S. Government Printing Office, 1974.

Symposium, "Is Privacy Obsolete? The Challenge to Medicine and Society," Prism, Vol. 2, June 1974 (Contributors: Sam J. Ervin, Arthur R. Miller, Lawrence L. Weed, John M. Rumsey, Alfred M. Freedman, Carmault B. Jackson, Ralph Crawshaw, Angela Roddey Holder, Alan F. Westin).

Symposium, "Silence is Golden, Or Is It? How Much Should the Doctor Tell, And to Whom?" Mental Hygiene, Vol. 57, Winter 1973, p. 21.

Szasz, Thomas S., "The Problem of Privacy in Training Analysis," Psychiatry: A Journal for the Study of Interpersonal Processes, Vol. 25, August 1962, p. 195.

"Testimony Heard on Insurer's Medical Data Files," Hospitals, Vol. 46, June 1, 1972, p. 22.

Thome, R., "Protection and Confidentiality of Medical Data: Efficient Data Protection Through Project-specific Combination of Methods," Medinfo 74, op. cit.

Thorns, Edward J., "Don't Be Afraid of Medical Records on Computers," Hospital Management, Vol. 102, October 1966, p. 31.

"Tucson Hospitals Refuse To Report Drug Abuses," Hospitals, Vol. 44, August 16, 1970, p. 180.

U.S. Department of Health, Education and Welfare, Appendix, Access Laws in the States, Report of the Secretary's Commission on Medical Malpractice, January 16, 1973.

Vidakovitch, John,"Are the Records of Mental Hospitals Privileged in Mental Incompetency Adjudications?" Wyoming Law Journal, Vol. 19, Winter 1965, p. 59.

Warshafsky, Ted M., "Approaches to Hospital Negligence," Case & Comment, September/October 1974, p. 12.

* Weinstock, Murray and Haft, Jacob I., "The Effect of Illness on Employment Opportunities," Archives of Environmental Health, Vol. 29, August 1974, p. 79.

* Westin, Alan F. and Baker, Michael A., Databanks in a Free Society: Computers, Record-Keeping and Privacy, New York, Quadrangle/New York Times Book Company, 1972.

"When a Credit Agency Asks for Medical Records," Medical World News, Vol. 13, September 1, 1972, p. 70.

"When May an MD Divulge What a Patient Tells Him?" Medical World News, Vol. 7, September 23, 1966, p. 44.

Willett, David E., "Medical Records, The Patient's Right To Information," California Medicine, Vol. 119, November 1973, p. 77.

Zachery, Mabel C., "Nurse - Personnel - Physician Symposium: Confidentiality of Medical Records," Archives of Environmental Health, Vol. 19, August 1969, p. 282.

FUTURE DEVELOPMENTS IN HEALTH CARE COMPUTERIZATION

Anderla, Georges, Information in 1985: A Forecasting Study of Information Needs and Resources, Paris, France, Organization for Economic Co-operation and Development, 1973.

Breslow, Lester, "Consumer-Defined Goals for the Health Care Systems of the 1980's," Technology and Health Care Systems in the 1980's, op. cit.

Collen, Morris F., Editor, Technology and Health Care Systems in the 1980's, Proceedings of a Conference, San Francisco, California, January 19-21, 1972, National Center for Health Services Research and Development, Health Services and Mental Health Administration, U.S. Department of Health, Education and Welfare,1972.

Greenblott, Bernard J. and Hsiao, Mu Y, "Where Is Technology Taking Us in Data Processing Systems?" Proceedings of the 1975 National Computer Conference, p. 623.

* Murnaghan, Jane H., "Health-Services Information Systems in the United States Today," New England Journal of Medicine, Vol. 290, March 14, 1974, p. 603.

Newitt, Jane B., "Health Care in a Changing Culture: Looking Toward the 1980's," Technology and Health Care Systems in the 1980's, op. cit.

Statskonsult AB, Solna, Sweden, "Data Processing Technology in 1980-85," January 1974 (English translation in Data Exchange, Diebold Europe, December 1974, p. 2.).

Wallace, June, "See Possibility of Having National Health Registry," Medical Record News, Vol. 41, February 1970, p. 23.

Withington, Frederic G., "Innovations in the Operation of Future Computers," Proceedings of the 1975 National Computer Conference, p. 633.

FUTURE DEVELOPMENTS IN HEALTH CARE

Analysis of National Health Insurance Proposals, Chicago, American Hospital Association, 1974.

Board of Governors Special Study Commission on National Health Insurance, "National Health Insurance: Principles Essential to a Successful Program," American College of Hospital Administrators, 1974.

Committee on Finance, United States Senate, Background Material Relating to Professional Standards Review Organizations, Washington, D. C., U.S. Government Printing Office, May 8, 1974.

Committee on Finance, United States Senate, National Health Insurance: Brief Outline of Pending Bills, Washington, D. C., U.S. Government Printing Office, 1974.

Crystal, Royal A., "PSRO: Functions and Problems in Confidentiality," Conference on the Confidentiality of Health Records, Key Biscayne, Florida, November 6-9, 1974.

Decker, Barry and Bonner, Paul, Editor, PSRO: Organization for Regional Peer Review, Cambridge, Massachusetts, Ballinger Publishing Company, 1973.

Goran, Michael J., M.D., et al., "The PSRO Hospital Review System," *Medical Care*, April 1975, Supplement, p. 1.

National Health Insurance, Hearings Before the Committee on Ways and Means, House of Representatives, Ninety-third Congress, Second Session; Washington, D.C., U.S. Government Printing Office, 1974 (Nine volumes).

"National Health Insurance: Which Way To Go?" *Consumer Reports*, February 1975, p.118.

* Massachusetts Medical Society, "PSRO's - Pros and Cons," *New England Journal of Medicine*, Vol. 290, June 6, 1974, p. 1319.

"Moving on Health Care," *Time*, April 15, 1974, p. 74.

PSRO - Issues and Answers, Office of Professional Standards Review, Department of Health, Education and Welfare, April 1974.

* Rivlin, Alice, "Agreed: Here Comes National Health Insurance," *New York Times Magazine*, July 21, 1974, p. 8.

Roberts, James A., "PSRO - A General Overview," *Journal of Clinical Computing*, Vol. 3, September 1973, p. 172.

Slee, Vergil N., M.D., F.A.C.P., "PSRO and the Hospital's Quality Control," *Annals of Internal Medicine*, July 1974, p. 97.

Somers, Anne R., *Health Care in Transition: Directions for the Future*, Chicago, Hospital Research and Educational Trust, 1971.

Turner, Judith Axler, "Health Report/HEW Begins Medical Review, A.M.A. Hospitals Mount Opposition," *National Journal Reports*, January 19, 1974, p. 90.

* Welch, Claude E., "Professional Standards Review Organizations - Problems and Prospects," *New England Journal of Medicine*, Vol. 289, August 9, 1973, p. 291.

Willett, David E., J.D., "PSRO Today: A Lawyer's Assessment," *New England Journal of Medicine*, February 13, 1975, p. 340.

COMPUTERIZATION AND CITIZEN RIGHTS ISSUES IN EUROPEAN COUNTRIES

* Anderson, J., "Kings Hospital Computer System (London)," in Morris F. Collen, *Hospital Computer Systems*.

* Anderson, J. and Forsythe, J.M., Editors, *Medinfo 74*, First World Conference on Medical Informatics, Stockholm, Sweden, August 5-10, 1974, Preprints of Papers.

Bottiger, Lars Erik, M.D., "The Danderyd Computer System for Total Regional Medical Care," Excerpt from Transactions of the Conference on Continuing Medical Education, State University of New York at Buffalo, June 3-6, 1971, *Journal of Medical Computing*.

Carroll, J.M. et al., *Personal Records: Procedures, Practices, and Problems*, A Study for the Privacy and Computers Task Force, Ottawa, Department of Communications/Department of Justice.

* *Computer Applications in the Field of Medicine*, Rome, Sperry-Univac International Executive Centre, 1970.

"Computer Information Systems in Health Care," (Series of six lectures based on Swedish and British experience), Sperry Univac, 1975.

Conference on Computer Applications in the Field of Medicine, Rome, Sperry-Univac International Executive Centre, April 2-4, 1974:

Bernard, Dr. D., "The Use of the Computer in Radiotherapy Planning," (Villejuif, France).

Côte, Dr. R.A., M.D., "An Approach to Medical Information Management," (Quebec).

Côte, Dr. R.A., M.D., "Computers in Clinical Laboratory Automation," (Quebec).

Harding-Smith, R., "Cost-Effectiveness for Decision Taking and Evaluation."

Harding-Smith, R., "Introduction to Syndicate Discussions."

Väänanen, Dr. I., M.D., "Computers in National and Regional Planning," (Helsinki).

Weixler, Dr. A., "The Place of the Computer in Health Care Delivery," (Graz, Austria).

White, D., "Characteristics of the Modern Health Service and Hospital," (London).

Conference on Computer Applications in the Field of Medicine, Rome, Sperry-Univac International Executive Centre, April 2-4, 1975:

Blainpain, Prof. J.E., M.D., "Characteristics of the Modern Health Service and Hospital," (Leuven, Belgium).

Hoogendoorn, Dr., D., "Patient Identification in a Health Data Base," (The Netherlands).

Peterson, Hans, M.D., "Security and Confidentiality in Health Care Information Systems," (Stockholm).

Van Egmond, Dr. J., "The Information System at the University Hospital of Gent."

Davis, Michael, "Toward a Medical Data Bank for a Total Population," (Israel) Datamation, November 1969, p. 257.

Department of Communications/Department of Justice, "Medical Databanks," Privacy and Computers, Ottawa, Information Canada, 1972, p. 72.

* Hall, P., "Karolinska Hospital Computer System (Stockholm)," in Morris F. Collen, Hospital Computer Systems.

McLachlan, Gordon and Shegog, Richard A., Editors, Computers in the Service of Medicine, London, Oxford University Press, 1968.

Maynard, Alan, Health Care in the European Community, Pittsburgh, University of Pittsburgh Press, 1975.

"Medical Information Processing: The KS Project," Stockholm, IBM, 1969.

Murray, D. Stark, Blueprint for Health, New York, Schocken Books, 1974.

Rapport de la Commission Informatique et Libertés, Paris, La Documentation Française, 1975.

Rapport de la Commission Informatique et Libertés--Annexes, Paris, La Documentation Française, 1975.

* Reichertz, P. "University of Hannover Hospital Computer System (Hannover)," in Morris F. Collen, Hospital Computer Systems.

Report of the Parliamentary Committee on Privacy, London, Her Majesty's Stationery Office, July 1972, pp.108-115.

Rowe, B.C., Editor, Privacy, Computers and You, London, National Computing Centre Ltd., 1972, pp. 73-81.

Rule, James B., Private Lives and Public Surveillance, London, Allen Lane, 1973.

Sauter, K., "The Patient Data Bank in a Medical Information System--Tasks, Requirements, Planning and Design," Methods of Medical Information, Vol. 12, No. 2, 1973, p. 113.

Schneider, W. et al., "IMS, Information Management System, As Data Base for Handling Medical Information," Sweden, Preliminary Technical Report.

"Second Interim Report of the Committee of Enquiry into the Protection of Privacy," Australia, 1974.

Sperry-Univac, "Medical Services of the Stockholm County Council."

Wakely, Gerald, Editor, "Medical Records Practice in New Zealand," Auckland.

Appendices

AMERICAN CIVIL LIBERTIES UNION
22 East 40th Street New York, N.Y. 10016 (212) 725-1222

July 15, 1974

To: Affiliates and Local Chapters
From: Alan F. Westin, Chairman, Privacy Committee

As you know, the Privacy Committee proposed to the ACLU National Board, and the Board recently adopted, an important policy statement on protecting the privacy of patient medical records, controlling the circulation of confidential medical information, and giving patients a right of access to their own medical records. These issues are going to become more important as plans for national health insurance move forward, as Professional Standards Review Organizations (PSRO) begin operations, and as medical records and registers are computerized in government databanks and private organizational files.

I am writing to you to ask whether you can report:

1. Any specific cases and issues in which breach of patient medical records or medical information has come to your attention. Clippings, briefs, or newsletter reports would be greatly appreciated; any costs of reproduction or mailing will be reimbursed.

2. Any examples of computerization of medical records in your area or state--by local or state government agencies or private institutions--that you have noted and taken any action about.

3. Any recent policy resolutions or staff representations (through letters or testimony) on these matters.

I would be most grateful if you could send along anything you have on these matters, or turn this letter over to the specialist in your affiliate who may follow such topics.

Many thanks for your assistance.

Sincerely,

Alan F. Westin

AFW;lc

P.S. Please send all replies to my home address: 960 Lincoln Place, Teaneck, New Jersey 07666.

Edward J. Ennis, Chairman, Board of Directors • Ramsey Clark, Chairman, National Advisory Council
Aryeh Neier, Executive Director Executive Department: Alan Reitman, Associate Director • Roger N. Baldwin, Executive Director Emeritus and International Work Advisor • Trudy Hayden, Brian Hellerman, Carol Jennings, Philip Ryan, Helene Toiv, Staff Associates

(100% recycled paper)

The Civil Liberties Review
22 East 40th Street 10th floor New York, New York 10016 (212) 689-8142 or 725-1222

Alan F. Westin
Editor

Walter J. Green
Managing Editor

October 31, 1975

To: Affiliate Directors

From: Alan F. Westin

In the summer of 1974, as chairperson of the ACLU Privacy Committee, I wrote to each ACLU affiliate asking for information about local cases or incidents involving violations of privacy in medical or health records. I obtained many excellent replies, and have followed these up with many of you.

Now, I am revising for publication a report on the civil liberties problems involved in manual and computerized files containing personal health data. The report covers whether medical or health data ought to be collected at all in a particular setting (employment, education, licensing, etc.); whether data collected is being held confidentially or is being disclosed to some persons inside the collecting organization or outside it who ought not to receive that information; and whether patients or other individuals who have disclosed their health data are given a right of access to their own records, if they seek that.

Could you tell me whether you currently have any incidents, protests, lawsuits, legislative activity, or other actions involving these issues? I am collecting episodes covering both manual records and computerized records.

I hope to feature an accurate and strong presentation of how people's rights in health data are being treated today, and I would be most grateful for any letters, clippings, legal papers, or other reports that you can send me.

Would you please address your replies to me at:

The Civil Liberties Review
22 East 40 Street, 10th Floor
New York, New York 10016

Many thanks for your help...

Editorial Committee: Derrick A. Bell Jr., Norman Dorsen, Robert F. Drinan, Thomas I. Emerson, Franklyn S. Haiman, Charles V. Hamilton, Michael Harris, Elizabeth Janeway, Robert Lekachman, Jessica Mitford, Harriet F. Pilpel, Frances Fox Piven, Inez Reid, David J. Rothman, André Schiffrin, Wilma Martinez Singer, Marvin E. Wolfgang, C. Vann Woodward

PROJECT ON MEDICAL RECORDS AND CITIZEN RIGHTS

Sponsored by the Institute for Computer Sciences and Technology, U.S. National Bureau of Standards

980 Lincoln Place, Teaneck, New Jersey 07666

Director
Alan F. Westin
Columbia University

INCIDENT REPORT

This Project, as part of its study of the ways in which automation of personal medical records may be affecting privacy, confidentiality, and patient access to records, is collecting accounts of incidents in which confidentiality of medical records has been violated, or attempts have been made to violate such confidentiality, either in manual or computer files.

Please describe any such incident that you know of in the space below. Either give it to the member of the Project that you are in contact with or mail it to the Project, at the address shown above. THANK YOU FOR YOUR HELP

Incident ______________________________

USE BACK OF SHEET IF NECESSARY FOR CONTINUATION ...

NAME OF PERSON CONTRIBUTING INCIDENT ______________________________

ADDRESS ______________________________

(The name of a person contributing an incident will only be used after contacting that person and obtaining agreement for such identification)

PROJECT ON MEDICAL RECORDS AND CITIZEN RIGHTS
Sponsored by the Institute for Computer Sciences and Technology, U.S. National Bureau of Standards
360 Lincoln Place, Teaneck, New Jersey 07666

Director
Alan F. Westin
Columbia University
Consultant
Michael A. Baker
Brooklyn College
City University of N.Y.
Research Staff
Jamie Broder
Richard Silberberg
Helena Toiv

FORM LETTER SENT TO MEDICAL ORGANIZATIONS

NAME AND ADDRESS

Under the auspices of the U.S. National Bureau of Standards, I am directing a research project on citizen-rights issues involved in the automation of medical records. We are looking at how patient records are currently kept in hospitals and clinics; how computerization is affecting such record-keeping and the circulation of patient data for repayment purposes and satisfaction of legal reporting duties; and the issues of privacy, confidentiality, and patient-access-to-records that are involved in new forms of medical services, from PSRO and national health insurance plans to the growth of large-scale medical research programs and medical registers. A brief summary of our project is enclosed.

We are writing to major professional organizations in the health field to obtain copies of any recent policy statements, reports, or other materials they may have issued on the topic of privacy and confidentiality of medical records, or on the uses of computerization in patient record keeping. We are also trying to collect accounts of recent episodes in which the confidentiality of personal medical records was violated, either for political or personal purposes or in order to advance governmental interests that were held to be superior to the privacy of the patient data.

I would be most grateful to learn what your group can report or may have published on these issues, and I know that readers of our study will want to have your views represented.

May we hear from you soon?

Sincerely yours,

Alan F. Westin

Alan F. Westin
Project Director

Medical Organizations Contacted

National Geriatrics Society

Lister Hill National Center for Biomedical Communication

Special Interest Group on Biomedical Computing

American Association of Medical Clinics

American College Health Association

Association of American Medical Colleges

Institute for Advancement of Medical Communication

Medical Correctional Association

Electronic Computing Health Oriented, Inc.

Institute for the Study of Health and Society

American Hospital Association

American Osteopathic Hospital Association

Association of Medical Superintendants of Mental Hospitals

Commission on Professional and Hospital Activities

Hospital Management Systems Society

Association of Life Insurance Medical Directors of America

American College of Physicians

American Society of Internal Medicine

American College of Obstetricians and Gynecologists

American Osteopathic Association

American Academy of Pediatrics

American Pharmaceutical Association

Drug Information Association

American Academy of Family Physicians

American Dental Association

National Association of Disability Examiners

Group Health Association of America

Blue Cross Association

National Association of Blue Shield Plans

American Academy of Health Administration

Assembly of Regional Health Planning Organizations

National Health Federation

American Association for Comprehensive Health Planning

American Medical Association

National Medical Association

American Medical Record Association

American Association for the Abolition of Involuntary Mental Hospitalization

Association of Mental Health Administrators

American Nurses Association

American College of Nursing Home Administrators

American Nursing Home Association

Citizens for Better Care in Nursing Homes, Homes for the Aged and Other After-Care Facilities

Medical Liberation Front

Association for Health Records

American School Health Association

Student American Medical Association

American College of Surgeons

American Venereal Disease Association

American Medical Women's Association

✓

Physicians Forum

American Psychiatric Association

American Public Health Association

Atomedic Research Center

Brain Information Service

Health Sciences Communications Association

American Association of Dental Schools

Living Bank

American Society for Hospital Pharmacists

Association of American Physicians and Surgeons

Association for Psychiatric Treatment of Offenders

National New Professional Health Workers

American Medical Writers' Association

American Geriatrics Society

American Chiropractic Association

International Society of Cybernetic Medicine

National Environment Health Association

American Academy of Medical Administrators

American Association of Medical Assistants

National Association of Private Psychiatric Hospitals

American Society for Medical Technology

2. PRIVACY DEFINITIONS, Developed by Dr. Willis H. Ware, RAND Corporation, September 23, 1975.

1. Privacy

The right of an individual to be left alone; to withdraw from the influence of his environment; or to be secluded, not annoyed, or not intruded upon. By extension, the right to be protected against physical or psychological invasion or against misuse or abuse of something legally owned by an individual or normally considered by society to be implicitly his property, e.g., one's home, one's solitude in a public place, the right to maintain something for private use or not available to others.

2. Personal privacy (or, information privacy)

(1) The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent data about them is communicated to or used by others; (2) the protection of an individual against harm or damage as a result of the operation of a record system; (3) the protection of an individual (or class of individuals) against unwelcome, unfair, improper, or excessive collection or dissemination of information or data about himself.

3. Personal (computer) privacy

The protection of one or more individual(s) from harm or damage as a result of abuse or misuse of personal information held on him in some record system.

4. Invasion of privacy

A violation of some aspect of privacy or personal privacy as defined above; in the record system sense explicitly, harm or damage to one or more individual(s) as a result of the operation of a record system.

5. Data privacy

The protection of data (typically in a computer-based system) for the sole use of one individual or organization, or by such others as the owner of the data may authorize, e.g., other individuals, organizations, agencies, or groups thereof.

6. Confidential(ity)

(1) Status accorded to data or information indicating that it is sensitive for some reason, therefore needs to be protected against theft or improper use, and must be disseminated only to individuals or organizations authorized (or privileged) to have it; (2) by extension, status (sometimes assured by law) accorded to data or information that reflects an understood agreement between the person furnishing the data and the person or organization holding it that prescribes the protection to be provided and the dissemination and use to be permitted; (3) a legally recognized relation between certain individuals (e.g., lawyer-client) that privileges communications between them from disclosure in court. (Sometimes, confidential information is legally required to be given in exchange for some benefit, privilege, right, or opportunity; sometimes it is voluntarily given.)

7. Computer security

The totality of measures required to (1) protect a computer-based system, including its physical hardware, personnel, and data against deliberate or accidental damage from a defined threat; (2) protect the system against denial-of-use by its rightful owners; and (3) protect data and/or programs and/or system privileges against divulgence to or use by unauthorized persons.

8. Network security

The totality of measures required to (1) protect a network including its physical hardware, personnel, and information or data against deliberate or accidental damage; (2) protect the network against denial of use by its rightful owners; and (3) protect the information or data in the network against divulgence by unauthorized recipients. It includes as a component computer security.

9. Data security

The safety of data from accidental or intentional but unauthorized disclosure, modification, or destruction.

10. Integrity (of data or systems)

The property of being what an item is thought to be, and therefore free of surprises.

11. Access control

The set of measures (including administrative, procedural, computer hardware, and computer software) that (1) limit access to a computer system to only individuals authorized to use it; and (2) limit access to information or data or programs within the system to only legitimate users authorized to have them.

12. Seepage

The flow of data or information whose access is presumed to be controlled by computer security safeguards, to unauthorized individuals who obtain it by circumvention or direct penetration of the system safeguards.

13. Linkage

The combination of data or information from one information system from that from another; in particular, the combination of computer files from two or more sources.

3. AMERICAN MEDICAL ASSOCIATION MODEL STATE BILL ON CONFIDENTIALITY OF HEALTH CARE INFORMATION

Draft 2-2-76

IN THE GENERAL ASSEMBLY

STATE OF ______________

A Bill

To Provide For Confidentiality
Of Health Care Information

Be it enacted by the People of the State of _______, represented in the General Assembly:

Section 1. This Act may be cited as the "Confidentiality Of Health Care Information Act".

Section 2. The purpose of this Act is to establish safeguards for maintaining the integrity of confidential health care information.

Section 3. For purposes of this Act --

(a) the term "health care provider" means any person, corporation, facility or institution licensed by this state to provide or otherwise lawfully providing health care services, including but not limited to a physician, hospital or other health care facility, dentist, nurse, optometrist, podiatrist, physical therapist or psycologist, and an officer, employee or agent of such provider acting in the course and scope of his employment or agency related to or supportive of health care services;

(b) the term "health care services" means acts of diagnosis, treatment, medical evaluation or advice or such other acts as may be permissible under the health care licensing statutes of this state;

(c) the term "confidential health care information" means information relating to a person's health care history, diagnosis, condition, treatment, or evaluation;

(d) the term "medical peer review committee" means a committee of a state or local professional medical society or of a medical staff of a licensed hospital, nursing home or other health care facility provided the medical staff operates pursuant to written bylaws that have been approved by the governing board of the hospital, nursing home, or other health care facility, or other organization of physicians formed pursuant to state or federal law and authorized to evaluate medical and health care services;

(e) the term "third party" means a person or entity other than the person to whom the confidential health care information relates and other than a health care provider.

Section 4. (a) Except as provided in subsection (b) or as otherwise specifically provided by law, a person's confidential health care information shall not be released or transferred without the written consent, on a consent form meeting the requirements of section 4 (d) of this Act, of such individual or his authorized representative. A copy of any notice used pursuant to section 4 (d), and of any signed consent shall be provided to the person signing a consent form.

(b) No consent for release or transfer of confidential health care information is required in the following situations: (1) to a physician, dentist, or other medical personnel for diagnosis or treatment of such individual in a medical or dental emergency, or (2) to medical peer review committees, or (3) to a State Insurance Department or other state agency for the purpose of reviewing an insurance claim or complaint made to such Department or other agency by an insured or his authorized representative or by a beneficiary or his authorized representative of a deceased insured, or (4) to qualified personnel for the purpose of conducting scientific research, management audits, financial audits, program evaluations, or similar studies, but such personnel shall not identify, directly or indirectly, any individual patient in any report of such research, audit, or evaluation, or otherwise disclose patient identities in any manner (the term "qualified personnel" means persons whose training and experience are appropriate to the nature and level of the work in which they are engaged and who, when working as part of an organization, are performing such work with published and adequate administrative safeguards against unauthorized disclosures), (5) by a health care provider, as reasonably necessary in the provision of health care services to a person, or in the administration of the office or practice or operation of a health care provider (as used herein, "administration" shall include, but not be limited to, purposes of: accreditation, reimbursement, liability risk management or appraisal,and defense or prosecution of legal actions), or (6) by an employer as reasonably necessary in the administration of a group insurance or workmen's compensation plan, or (7) upon the filing of a claim for insurance benefits, between third party insurers to determine their relative rights and obligations concerning the individual's entitlement or the amount or kind of insurance benefits, when the policy of insurance obtained by the individual provides for obligations by more than one insurer with respect to a claim for benefits.

The release or transfer of confidential medical information under any of the above exceptions shall not be the basis for any legal liability, civil or criminal, nor considered a violation of this Act.

(c) Third parties receiving and retaining an individual's confidential health care information must establish at least the following security procedures: (1) limit authorized access to personally identifiable confidential health care information to persons having a "need to know" such information; additional employees or agents may have access to such information which does not contain information from which an individual can be identified; (2) identify an individual or individuals who have responsibility for maintaining security procedures for confidential health care information; (3) provide a written statement to each employee or agent as to the necessity of maintaining the security of confidential health care information, and of the penalties provided for in this Act for the unauthorized release, use, or disclosures of such information; receipt of such statement shall be acknowledged by such employee or agent signing and returning same to his employer or principal and the employer or principal shall furnish his employee or agent with a copy of the signed statement, and shall retain the original thereof; (4) take no disciplinary or punitive action against any employee or agent who brings evidence of violation of this Act to the attention of any person or entity.

(d) Consent forms for the release or transfer of confidential health care information shall contain, or in the course of an application or claim for insurance be accompanied by a notice containing, at least the following:

(1) the need for and proposed use of such information;

(2) a statement that all information is to be released or indicating the extent of the information to be released, and

(3) a statement that such information will not be given, sold, transferred, or in any way relayed to any other person or entity not specified in the consent form or notice without first obtaining the individual's additional written consent on a form stating the need for the proposed new use of such information or the need for its transfer to another person or entity, and,

(4) a statement that such consent applies only to the release or transfer of confidential health care information existing prior to the date such consent is signed, except that when such consent is given in the course of an application or claim for insurance it shall also apply to medical information existing at any time during the period of contestability provided for in the policy and during periods of ongoing proofs of loss during a claim.

Section 5. (a) Upon occurrence of an action or decision of any third party, which adversely affects a person, and which is based in whole or in part upon his confidential health care information, including, but not limited to, the following actions or decisions: (1) denial of an application for an insurance policy; (2) issuance of an insurance policy with other than standard and uniform restrictions; (3) rejection in whole or in part of any claim for insurance benefits; (4) denial of an employment application or termination of employment when such denial or termination is for health reasons; and upon the written request of such person or his authorized representative (or, if such person is deceased, then his heir or beneficiary or their authorized representative or his estate), a third party shall transfer all of such person's confidential health care information in its possession to a physician designated in such written request.

Prior to making such transfer, a third party may require payment of its actual cost of retrieval, duplication and forwarding of such information.

(b) A physician receiving confidential health care information pursuant to (a) above, may review, interpret and disclose any or all of such information to the person at whose request such information was transferred, as said physician deems in his professional judgment to be in the best interests of the person to whom such information relates.

(c) After reviewing his confidential health care information pursuant to this Section, a person or his authorized representative may request the third party to amend or expunge any part he believes is in error, or request the addition of any recent relevant information.

Upon receiving such a request, the third party shall notify the health care provider who initially forwarded such information to the third party, and when such health care provider concurs with such request, the third party shall return such information to that health care provider for modification. Prior to making such return, a third party may require payment of its actual cost of notice, duplication, and return of such information. Except upon court order, the third party shall not itself modify such information. A person after requesting and reviewing his confidential health care information shall have the right, in any case, to place into the file a statement of reasonable length of his view as to the correctness or relevance of existing information or as to the addition of new information. Such statement or copies thereof shall at all times accompany that part of the information in contention.

Section 6. (a) (1) Except as provided in subparagraph (2) hereof, confidential health care information shall not be subject to compulsory legal process in any type of proceeding, including, but not limited to, any civil or criminal case or legislative or administrative proceedings or in any pre-trial or other preliminary proceedings, and a person or his authorized representative has a privilege to refuse to disclose, and to prevent a witness from disclosing, his confidential health care information in any such proceedings.

(2) The exemption from compulsory legal process and the privilege provided in subparagraph (1) above shall not apply when:

(A) an individual introduces his physical or mental condition, including, but not limited to, any allegation of mental anguish, mental suffering or similar condition as an element of his claim or defense, provided that a claim for damages or other relief for "pain and suffering" based solely on one's physical condition does not constitute the introduction of one's mental condition into issue and the exemption and privilege shall apply in such situation as to those portions of one's confidential health care information relating to mental condition.

(B) the individual's physical or mental condition is relevant regarding the execution or witnessing of a will or other document;

(C) the physical or mental condition of a deceased individual is introduced by any party claiming or defending through or as a beneficiary of such individual;

(D) in a civil or criminal commitment proceeding, a physician, in the course of diagnosis, treatment, or medical evaluation of an individual, determines that an individual is in need of care and treatment in a hospital or any other health care facility which is deemed by the individual's physician to be appropriate for mental illness;

(E) a judge finds that an individual, after having been informed that the communications would not be privileged, has made communications to a psychiatrist in the course of a psychiatric examination ordered by the court, provided that such communications shall be admissible only on issues involving the individual's mental condition;

(F) in any court proceeding, including an ex parte hearing, it is demonstrated on a prima facie basis to the court that the individual's physical or mental condition is of an imminent and serious danger to the physical or mental health of another person, or to the security of the United States, or

(G) in any action by an individual pursuant to Section 9 of this Act, or in any policy action brought by an individual against his insurance carrier, or by the carrier against an insured, or in any other action by an individual wherein it is demonstrated to the court that such confidential health care information is relevant and material then such court may issue an order compelling production of such information.

(b) The exceptions contained in items (A) through (G) of subparagraph (2) above are not intended to preclude the exemption or privilege described in subparagraph (1) above in any pretrial or trial proceedings under the Divorce Act of this State unless the individual or witness on his behalf first testifies as to such confidential health care information.

Section 7. (a) Notwithstanding other provisions of this Act, health care providers may make confidential health care information available to medical peer review committees without authorization.

(b) Confidential health care information before a medical peer review committee shall remain strictly confidential, and any person found guilty of the unlawful disclosure of such information shall be subject to the penalties provided in this Act.

(c) Except as otherwise provided in this Section, the proceedings and records of medical peer review committees shall not be subject to discovery or introduction into evidence. No person who was in attendance at a meeting of such committee shall be permitted or required to testify as to any matters presented during the proceedings of such committee or as to any findings, recommendations, evaluations, opinions or other actions of such committee or any members thereof.

Confidential health care information otherwise discoverable or admissible from original sources is not to be construed as immune from discovery or use in any proceeding merely because they were presented during proceedings before such committee, nor is a member of such committee or other person appearing before it to be prevented from testifying as to matters within his knowledge and in accordance with the other provisions of this Act, but the said witness cannot be questioned about his testimony or other proceedings before such committee or about opinions formed by him as a result of said committee hearings.

(d) The provisions of sub-section (c) above limiting discovery or testimony do not apply in any legal action brought by a medical peer review committee to restrict or revoke a physician's hospital staff privileges, or his license to practice medicine, or to cases where a member of the medical peer review committee or the legal entity which formed such a committee or within which such committee operates is sued for actions taken by such committee, provided that in any such legal action personally identifiable portions of a person's confidential health care information shall not be used without written authorization of such person or his authorized representative or upon court order.

(e) Nothing in this Act shall limit the authority, which may otherwise be provided by law, of a physician licensing or disciplinary board of this State to require a medical peer review committee to report to it any disciplinary actions or recommendations of such committee, or to transfer to it records of such committee's proceedings or actions, including confidential medical information, or restrict or revoke a physician's license to practice medicine, provided that in any such legal action personally identifiable portions of a person's confidential health care information shall not be used withour written authorization of such person or his authorized representative or upon court order.

(f) No member of a medical peer review committee nor the legal entity which formed or within which such committee operates nor any person providing information to such committee shall be criminally or civilly liable for the performance of any duty, function, or activity of such committee or based upon providing information to such committee; provided such action is without malice and is based upon a reasonable belief that such action is warranted.

Section 8. (a) Civil Penalties - Anyone who violates provisions of this Act, may be held liable for special and general damages, and punitive damages may be granted for malicious violation of this Act.

(b) Criminal Penalties - Anyone who intentionally and knowingly violates provisions of this Act shall, upon conviction, be fined not more than $5,000, or imprisoned for not more than one year, or both.

(c) The civil and criminal penalties above shall also be applicable to anyone who obtains an individual's confidential health care information through the commission of a crime.

Section 9. A person or his authorized representative shall have the right, when there is an unreasonable refusal to change the records as provided in Section 5, to seek through court action the amendment or expungement of any part of his confidential health care information in a third party's possession which he believes is erroneous.

Section 10. Attorney's fees and reasonable costs may be awarded, at the discretion of the court, to the successful party in any action under this Act.

Section 11. Any agreement purporting to waive the provisions of this Act is hereby declared to be against public policy and void.

Section 12. If any provision of this Act is held by a court to be invalid, such invalidity shall not affect the remaining provisions of this Act, and to this end the provisions of this Act are hereby declared severable.

Section 13. This Act shall become effective _________(one year) from the date of being signed into law.

4. IBM MEDICAL DEPARTMENT MANUAL: PRIVACY POLICY

IBM **Medical Department Manual**

Section: Privacy

Index: 1-5
Page: 2
Issued: 6/15/75

GENERAL. The IBM Company adheres to ethical, legal and confidential standards in the handling of medical records of its employees. Prior approval of the employee (signed Medical Information Release form) will be obtained before either disclosing or seeking confidential medical information, except in an emergency or where such disclosure is required by law. Management should notify the involved employee and the responsible Medical Department of the circumstances necessitating securing confidential medical information. Neither management nor Personnel will request or accept an employee's medical record. Access to confidential medical records is limited to the IBM Medical staff and department personnel under their immediate supervision.

Upon request to the Medical Department, employees will be permitted access to certain materials in their medical records to which they have a legal right (such as OSHA data, Public Health data) and factual medical data such as laboratory tests, blood pressures, physical findings (but not including subjective or interpretive data, or medical opinions). The employee does not have right of access to the primary active working part of the medical record which contains notes by the IBM Medical staff, or to information obtained from the patient which the IBM physicians/nurses intended solely for their own use, or to third-party communications, including information from managers. However, at the request of an employee or in the normal course of their duties, IBM Medical personnel will discuss or interpret this information concerning that employee on an individual case basis. The custodian of medical records will take all reasonable precautions to assure the accuracy and reliability of the data, and will correct any erroneous data. Medical personnel will be available to interpret medical data from the record for the employee.

As appropriate, managers, Personnel, and employees, will be provided with recommendations concerning medical limitations pertaining to particular job requirements, but medically confidential information will not be provided to managers or Personnel without the prior consent of the employee.

Employees must provide medical information to IBM when the Company has a need to know such information in order to carry out its policies regarding job assignment, benefits, absenteeism, international assignments, security, Workmen's Compensation, etc.

Managers will not consult an employee's private physician(s) concerning medical problems, and should resolve with the IBM Medical staff any questions concerning proper action. When managers require verification of facts with medical implications, they should request that the employee have the appropriate information sent to the Medical Department for interpretation. Managers should recognize that our posture concerning confidentiality may result in delay in the resolution of some problems.

MEDICAL RECORDS. Medical records are confidential and private. An employee has right of access to certain materials in his occupational medical records. Through medical information releases the employee also has some control over what material in his/her medical record can be used, to whom it will be disseminated, and for what purpose.

All medical information except details of first-aid visits concerning the individual employee is to be maintained in one medical record. No location will maintain dual medical records on an individual employee. There will be no personally identifiable separate medical record-keeping system. Individuals or legitimate authorities acting in their behalf, by presenting themselves at the medical records location, may have access to certain information kept in their medical records, and may learn how it is to be used. Accessible kinds of information are defined below under "levels". Identifiable information about an individual obtained for business purposes cannot be used or made available for other purposes without the individual's consent. (See section on Voluntary Health Screening Examination Program in this index.) Where private medical advice is sought, and when there is no performance impact and the law permits, Medical is under no obligation to notify management of restrictions reflecting the presence of a medical condition.

The individual responsible for the medical-record will correct any erroneous data contained in the medical records when such error is identified and documented. The responsible medical department must take all reasonable precautions to assure the accuracy and reliability of the data, and take precautions to prevent misuse of the data.

This medical-record system philosophy involves a concept of levels of information and accessibility:

LEVELS.

Level I	Material to which the employee has legal right, such as Occupational Safety and Health Act data, Public Health data, and other materials stipulated by law.
Level II	Medical data which an employee should have the right to examine and correct if necessary. This would include factual medical data that is not subject to opinion or subjective interpretation, such as laboratory tests, blood pressures, physical findings, Voluntary Health Screening Examination Program Results.
Level III	Material to which the employee does not have right of access. The primary active working medical record containing notes by the physician/nurse, information obtained from the patient, or information obtained with the patient's consent, which the physician intended solely for his/her own use in the management of the case--third-party letters, consultations, information from

management, or copies of physicians' and hospital reports, psychological test data and interpretations.

An IBM physician or nurse will, at the employee's request, release and discuss with the employee the first two levels of medical information from a medical record. The employee does not generally have right of access to material classified as Level III. However, at the request of an employee or in the normal course of their duties, IBM Medical personnel will discuss or interpret Level III materials concerning that employee on an individual case basis. Care must be taken to limit disclosure of Level III material by IBM Medical personnel.

RELEASES. An employee's informed consent (Medical Information Release) (see Index 5-2) is required before medically confidential information is released to third parties (insurance companies--including our own carriers--governmental agencies, and others), except as required by law, in which case if feasible the employee should be notified of the release of this information. It is advisable to contact the employee if there is any question concerning understanding, specificity, and possible consequences of release of medically confidential material.

A Medical Information Release form must be used for both seeking and giving information. Basically, informed consent specifies the purpose, recipient, source of information requested, is voluntarily executed by the involved employee, is restricted usually to past and present events, and is revokable by the employee.

Except in cases of emergency, releases are appropriate for personal physician contact. Non-solicited information from personal physicians is the responsibility of the personal physician, and such information should be used with discretion within IBM. It is presumed that the sender has been given permission to release this information and that he/she may be questioned by IBM for clarification of the information received. Situations wherein the personal physician is also the IBM physician require additional sensitivity.

RELEASE FORMS. (Absence) A sample of the form to secure medical information from the personal physician of the employee is included in Index 5-2. They are initiated by management but eliminate the manager as middle person in the response; their use is recommended. Managers should notify the Medical Department and the employee of the circumstances necessitating the request for releases. Through use of Medical Department self-addressed envelopes, etc., provision must be made to allow the employee to have medically confidential information sent directly to the Medical Department. Areas or Divisions developing their own forms for this purpose or other uses with medical implications should inform the Office of the Corporate Medical Director. Location Medical Departments developing such forms must work through their Divisional or Area Medical Department for consultation and approval.

SPECIAL PROGRAMS. In certain governmental programs regarding handicapped, etc., the law may require release of data to appropriate IBM personnel or governmental agencies. If individual identification is requested, the specific legal requirements should be clarified by IBM legal counsel prior to release of information.

DRUG AND ALCOHOL ABUSERS. There is a Corporate program regarding handling cases where the job is impacted. When Medical involvement is management initiated and where performance is impacted, then it should be made clear to the employee that Medical must advise responsible management of the basic illness so that the proper medical program can be instituted. Where private medical advice is sought, and when there is no performance impact and the law permits, Medical is under no obligation to notify management of restrictions reflecting the presence of a medical condition.

APPLICANTS. Medical will not reveal diagnoses or other confidential medical information to managers or Personnel without prior approval from the applicant. If the applicant has a history of drug or alcohol abuse, he/she should be counseled to allow Medical to notify management. The possibility of appropriate medical follow-up should be explained to the applicant. The applicant must be notified that we will inform managers and Personnel of job restrictions.

Class III applicants will be informed of their problem by the examining physician. The responsible IBM Medical Department will notify Personnel of the Class III designation. In these cases regulations on employment of the handicapped may apply. The Employment Manager should consult with the responsible IBM Physician on the appropriate course of action, which may include advice on how best to communicate the employment decision to the applicant. Each case should be handled on an individual basis, with the utmost sensitivity to the applicant's perception of the decision. It is extremely important that the file be carefully and thoroughly documented.

The IBM Medical Department will notify Class II applicants of their medical problems and job restrictions and also of the fact that managers and Personnel, or other persons in the Company with a need to know, will receive a copy of the job restrictions.

When special tests such as urine chromatography for drugs are carried out, it is necessary to inform the applicant what the test is for and also that there may be some legal requirement to report positive results.

Governmental regulations may necessitate notifying applicants when they have a handicap classification.

LEGAL REQUIREMENT. Certain agencies such as Workmen's Compensation Boards, Public Health agencies, Occupational Safety and Health Act, and other regulatory agencies operating under other laws, may have legal right to confidential material with group or, at times, individual identification.

In other instances, they may have the legal right to request such information but only reeive it with the approval of the affected individuals. Medical Departments should seek the help of IBM legal counsel for clarification to avoid erroneous interpretation.

HAZARDOUS OR COMPLEX SITUATIONS AND CASES. There are situations where a physicial or emotional health problem seriously impacts performance or creates a hazard. In such instances, when ethically appropriate, restrictions necessary to protect the individual, his/her co-workers, and the Company should be instituted. The employee should be strongly counseled to allow Medical to release the minimum of medically confidential material so that appropriate instructions can be given to managers or first-aid teams (e.g., diabetic or epileptic employees). It should be pointed out that it is for the benefit of the employee and his/her co-workers that we wish to release minimal amounts of information, and that it is also his/her responsibility to the Company to allow us to take some reasonable action. Instructions to first-aiders on appropriate first-aid assistance may compromise some aspects of medical confidentiality, but it would be an extremely rare situation that would necessitate revealing a diagnosis.

VERIFICATION OF MEDICAL INFORMATION. Managers may occasionally request the Medical Department to verify certain statements of fact or conditions with medical overtones which an employee presents to them (verifying that a visit was made to an emergency room or doctor's office, or that a physician did, in fact, make certain recommendations that could affect attendance or job requirements). It is management's responsibility to request that the employee procure statements or provide documentation which can then be sent directly to the Medical Department for interpretation.

HOME CONTACT (INCLUDING TELEPHONE CALLS) BY MANAGERS. These are administrative and not Medical Department issues. Only in an emergency should a member of the Medical staff visit or contact the home of an employee without consent, and then only after consideration of other options (local authorities, family contacts, personal physician, etc.), since even appropriate action could be considered invasion of privacy or harassment.

Contact with family members should be made only with permission of the employee, except in emergency situations or in cases of a psychological state where understanding may be lacking (See Index 4-2).

COSULTATIONS. When seeking consultation, the IBM practice regarding the Company's right to request consultation and the employee's responsibility for allowing us to receive a report of the consultation should be explained to the employee. Reference may be made to the About Your Company booklet: "The company, in deciding whether or not you are entitled to benefits, may require an examination by a physician of the company's choice. The company's decision is final."

TAPE RECORDERS. Tape recorders are not to be used for recording employee-physician conversations. The responsible Medical Director's approval and the employee's approval are required when recordings, films, or TV tapes are proposed to be made for educational purposes.

INTERNATIONAL ASSIGNMENTS. (Refer to Index 2-5.) The international assignment physical examination program is designed to benefit the employee and his/her family, and protect them from difficult medical situations when on international assignment. The IBM Medical Departments may require certain medical information concerning the employee or his/her family members so that proper administrative recommendations can be made to management. It is the responsibility of the employee and family members to provide required information to the IBM Medical Departments. IBM must be especially sensitive concerning handling confidential medical information about individuals who are not IBM employees.

As outlined under the International Assignment Transfer Instructions, an individual and family members (of legal age) may individually be given medical summaries regarding their individual medical status. IBM Medical Departments must be alert to realize that medical information regarding an adult (and certain information concerning minors) is restricted to the individual concerned. Discretion and sensitivity must be used to avoid potentially embarrassing situations to the individual or family members, and to the IBM Company.

MEDICAL CARE ORGANIZATIONS. In future years we anticipate that both our Medical and Benefits programs will be impacted by Health Maintenance Organizations, Foundations for Medical Care, etc., as regards their "total care" of the patient. The relationship between each HMO, Foundation, etc., the employee, and IBM must be understood to avoid conflict.

BENEFITS PROGRAM. The proper administration of the Total and Permanent Disability Plan necessitates divulging some medically confidential information at the Corporate level. Medical confidence is maintained up to the final levels of decision-making, at which time an IBM physician is available to release and interpret only the material necessary for a decision to be made.

VOLUNTARY HEALTH SCREENING EXAMINATION PROGRAM. In keeping with the intent of the Voluntary Health Screening Examination Program and IBM concepts of medical data privacy and confidentiality, information obtained from the examination is not to be used to restrict an employee without his or her prior approval.

Information in the medical data bank is confidential and, except as required by law, its use is governed by these privacy guidelines.

Correction of erroneous material in the data bank is required when documented. Correction of material in the data bank should be discussed with the Medical Data Center personnel. As originally intended, release of the VHSEP printout continues to be restricted (see next paragraph) to licensed practitioners of medicine. Release of the printout (with the employee's approval) to other health organizations or individual practitioners would depend on acceptable practice in the community.

Routinely employees will not be given the VHSEP printout, but upon specific request, a copy of the printout must be provided to them. Printouts are considered Level II material.

MEDICAL/PERSONNEL REVIEW COMMITTEE MEETINGS. These are conducted at many locations. Medical personnel must be aware that in such meetings there is the possibility of medically confidential information being discussed or divulged. Medical must be careful not to divulge any unreleased confidential material.

MEDICAL-RECORD UPDATE. To adhere to IBM's philosophy concerning medical records, it is important that review of restrictions as compared to current medical status of the employee be done periodically to eliminate unnecessary or outdated restrictions. When accurately documented objective information reveals erroneous material in the medical records, including computer records, correction is required. Medical records are not to be purged, but incorrect items are left intact and the error noted, and a corrected statement made.

MEDICAL-RECORD RETENTION. Medical records on active employees should be retained intact without time limits. Stored records on former employees should be maintained according to Corporate Headquarters Record Retention Standards or until the statute of limitations expires, or the legal requirements of OSHA or other governmental agencies expire, depending on which comes last. When medical records are sent to storage, they will be handled in accordance with the holder's usual methods of storing records.

EXHIBIT 13

IBM CONFIDENTIAL

MEDICAL INFORMATION REQUEST RELEASE

(Use to Secure Information)

The purpose of obtaining medical information is to assess an individual's health status as it relates to the work environment, assist in rehabilitation, and determine eligibility for sickness and accident benefits. This information will be used by IBM medical personnel in a confidential manner and will not be released. unless required by law.

To ______________________________
(Print Physician's or Hospital Name)

____
(Address)

____
(Area Code and Telephone Number)

I, ______________________________, hereby authorize and
(Print Employee's Name)
request you to release to the IBM Corporation Medical Department a summary of hospital and/or medical records in your possession concerning my illness and treatment during the period commencing ______________
(Date)
as requested by that department.

______________________________ (IBM Location)

______________________________ (Address)

Signed ______________________________ Date ______________

Witness ______________________________ Date ______________

Previous to use by the IBM Medical Department the individual may limit or withdraw this authorization by contacting the IBM Corporation Medical Department or his/her manager.

cc: Employee

IBM CONFIDENTIAL

MEDICAL INFORMATION RELEASE

(Use to Release Information from IBM)

This information should be used in a confidential manner and unless required by law is not intended for use by others than the recipient.

TO IBM MEDICAL DEPARTMENT:

I, ______________________________, hereby authorize you to release
(Print Employee's Name)

to ____
(Print Name of Physician or Hospital)

____
(Address)

____
(Area Code and Telephone Number)

a summary of my medical records in your possession pertaining to

______________________________, and covering the period
(Subject or Illness)

from ______________________ through ______________________
(Date) (Date)

Signed ______________________________ Date ______________

Witness ______________________________ Date ______________

Previous to compliance by the IBM Medical Department the individual may limit or withdraw this authorization by contacting the responsible IBM Medical Department in writing.

cc: Employee

IBM **CONFIDENTIAL**

PHYSICIAN'S REPORT TO MEDICAL DEPARTMENT

To the Attending Physician:

You are requested to complete section C of this form and forward it in the accompanying pre addressed envelope. The information supplied will be used in a confidential manner to assist in rehabilitating your patient and in assessing his eligibility for benefits under the company's Sickness and Accident Plan.

The activities of the company's medical department in rehabilitation are carried out in close co-operation with the attending physician.

Medical Director

SECTION A · To be completed by the employee's manager

Mr.
Mrs.
Miss ______________ surname ______________ given names ______________ employee serial no.

ADDRESS ______________

DEPT. NO. ______________ OCCUPATION ______________ LENGTH OF SERVICE ______________

MANAGER ______________ FIRST FULL DAY OF ABSENCE ______________

This is first ☐ / supplementary ☐ report Today's Date ______________

SECTION B · To be completed by employee (PLEASE PRINT OR TYPE)

TO ______________ physician's name ______________ full address ______________ telephone no.

I hereby authorize you to supply the information requested ______________ employee's signature

---

SECTION C Attending Physician's Report

1. Date of examination on which this report is based ______________ 19 ____
2. Diagnosis, including any complications ______________

GENERAL

Operation (if any) ______________ Date ______________

3. Is disability the result of: ILLNESS NON-INDUSTRIAL ☐ INDUSTRIAL ☐
   INJURY NON-INDUSTRIAL ☐ INDUSTRIAL ☐

REHABILITATION

4. When in your judgement should employee be able to return to work?
   a) to regular occupation full time ______________ 19 ____
   b) to regular occupation part time ______________ 19 ____
   c) to a lighter occupation full time ______________ 19 ____
   d) to a lighter occupation part time ______________ 19 ____

N.B. IBM tries to arrange suitable interim placement when indicated, in the belief that it is in the employee's best interests to resume work, even if limited, as soon as physically able.

REMARKS AND WORK LIMITATIONS ______________

5. Do you wish the company's Medical Director to contact you with respect to the rehabilitation of your patient? YES ☐ NO ☐

DATE ______________ 19 ____ ______________ signature M.D.

Address (if other than in Section B) ______________

5. HEW DRAFT POLICIES ON CONFIDENTIALITY FOR PROFESSIONAL STANDARDS REVIEW ORGANIZATIONS, 1975

For the purposes of this paper, the following definitions shall apply:

A. PSRO Data and Information
Data and information which is acquired and/or generated by any PSRO.

B. Individual PSRO Data and Information
Computer or hard copy data and information identifiable to a specific individual.

C. Identifiable Data of Information
Data and information collected, generated or aggregated on a particular individual which identifies that individual either explicitly or by implication.

D. Privileged Data and Information
Medical data and information identifiable to an individual patient, data and information indicating patterns of health care practices identifiable to individual health care practitioners, records of PSRO determinations identifiable to individual health care practitioners and data and information collected and/or generated for medical care evaluations studies as defined in department regulations and guidelines.

E. Monitoring
The review and appraisal of PSRO functions.

F. Evaluation
The determination of program effectiveness and the impact of the PSRO program on quality of care and utilization of services.

G. PSRO Review System
A system comprised of the PSRO and all supporting components which assist the PSRO in the review process or are furnished PSRO data for administrative purposes under Titles 18, 19, and 5 of the Social Security Act. The system may include (but is not limited to):

1. Hospital(s) if delegated review authority
2. PSRO review coordinator(s)—individuals responsible for carrying out PSRO activity within the health care facility
3. Medicare Intermediary(s)
4. Independent Health Data System(s), e.g., discharge abstract service
5. The PSRO
6. Medicaid State Agencies and Fiscal Agents
7. PSRO Contractors (any independent vendors providing data or data processing services to the PSRO)
8. Medicare Carriers
9. Other PSROs
10. DHEW
11. PSRO Support Centers
12. State PSRO Council
13. State Maternal and Child Health Agencies (Title V)

H. Health Care Practitioners
Physicians and other health care practitioners who are reimbursed for services through Medicare, Medicaid, or Maternal and Child Health programs.

I. Health Care Facilities
Organizations and institutions involved in the delivery of health care services (e.g., hospitals, nursing homes, outpatient facilities, etc.)

J. Sanction Proceedings
Procedures under Section 1157 and 1160 of the Social Security Act commencing with the forwarding of a sanction report by the PSRO under Section 1157.

K. PSRO Deliberations
Minutes of meetings, notes, comments, or other forms of recordings which evidence internal PSRO discussions pertaining to review or sanctions.

Policy Statements

1. Notification to Public

The PSRO must establish and implement a procedure for public notification of the existence, scope and purposes of PSRO data system.

2. Notification to Patients, Practitioners, and Providers

The PSRO must establish and implement procedures to inform individual patients, health care practitioners and health care facilities on whom PSRO data and information has been or is being collected as to:

a. the name, title and address of the person immediately responsible for the PSRO data system
b. those who will have access to the file
c. the circumstances under which and the purposes for which PSRO data and information will be disclosed

The procedures for notification should be administratively efficient, but provide at a minimum for general notification of the above.

3. Obtaining Access to own PSRO Data and information

Subject to restrictions on disclosure of PSRO deliberations (see #19), patients, health care practitioners and health care facilities must be allowed access, upon request, to their individual PSRO data and information for purposes of ascertaining the accuracy of that data and information. The PSRO must establish and implement procedures to verify the accuracy of the data and information; the data and information to be accessed shall not be physically removed and/or transmitted outside of the PSRO.

4. Patient Access: Special Procedures

When a patient requests access to PSRO data and information under paragraph 3 above, the physicians of record must be notified in writing at least ten working days prior to patient access. The patient will not require physician authorization to access his individual PSRO data and information nor can the physician prevent patient access to the data and information. However, if upon receiving notification of intended patient access, a physician of record objects to the release of such information without clarification, he or his designee may be present when the patient accesses his individual file to make such clarification.

5. Limitation on Data Collection

The PSRO or any agent, organization or institution acting on its behalf as a collector, processor and/or reviewer of information must limit the collection of PSRO data and information to that necessary for the purposes of PSRO review and/or evaluation.

6. Limitation on Data Access

Each component of the PSRO review system will have access only to that PSRO information and data necessary to carry out its functions within the system.

7. Limitations on Establishment of a National PSRO Data Base

Privileged data and information shall not be stored in a manner which constitutes creation of a national PSRO data base.

8. Codification of Personal Identifiers

Identification of individual patients, health care practitioners and health care facilities on PSRO generated reports and forms must be in a coded form except for verification purposes as provided for in paragraph 3 above. Index files containing cross reference of codes to names of patients, practitioners and facilities will be maintained in a secure manner within the PSRO review system.

9. Purgation: Computer Files

Computer files may be maintained indefinitely; however, each PSRO must purge such files of all personal identifiers as soon as such identifiers are no longer necessary (guidelines recommending time periods will be developed) for purposes of review, appeals, program monitoring and program evaluation.

10. Purgation of Hard Copy

Privileged information maintained in hard copy must be purged when that information has served the specific purpose for which it was generated.

11. Responsibility for Confidentiality Vested in a Single Individual

A single individual within the PSRO must be assigned the responsibility for maintaining the confidentiality of PSRO data within the PSRO review system and for the notification to DHEW of any breaches of confidentiality within the review system. A plan for implementing this responsibility will be submitted to DHEW for approval.

12. Responsibility of Officers and Employees

All officers and employees of the PSRO and components of the PSRO review system must be made aware of their responsibility to maintain the confidentiality of PSRO data and information and of the legal penalties which may be assessed for unauthorized disclosure of PSRO data or information (*i.e.*, fined not more than $1,000 and/or imprisoned not more than six months, under section 1166(b) of the Social Security Act).

13. Authorized Access: Requirements

An individual officer or employee of a component of the PSRO review system may not be authorized access to privileged PSRO data and information until that individual:

a. Has completed a training program in the handling of such data and information pursuant to paragraph 14 below; and

b. Has signed a statement indicating that: (1) the individual recognizes his responsibility to hold the data in confidence, and (2) is aware of the legal penalties which may be assessed for unauthorized disclosure of such data and information (*i.e.*, fined not more than $1,000 and/or imprisoned not more than six months).

14. Training Requirements

It is the responsibility of the PSRO to provide an ongoing program of training in the handling of PSRO privileged information for those officers and employees of PSRO review system components authorized to handle such data.

15. Access to Hard Copy

Each access to privileged data and information which requires removal of the data or information outside of a PSRO review system component, must be recorded in such a manner as to indicate what material was accessed, purpose, when, by whom, where the material was taken, and when returned. A separate log shall be kept recording access to the index code file (see paragraph 8). This log shall indicate the purpose of access, when, and by whom.

16. Disclosure: Licensing Boards

Copies of sanction reports forwarded to the Secretary of DHEW under Section 1157 of the Social Security Act may at the same time be forwarded to state licensing boards. However, the practitioner or facility must be notified in writing at least 15 working days prior to disclosure to permit the submission of a statement to accompany the disclosed sanction report. If the licensing board has been forwarded a copy of a sanction report, the PSRO shall inform the licensing board of the DHEW determination within a reasonable time after determination is made.

17. Disclosure: Civil Litigation

Subject to regulations governing administrative hearings under section 205(b) of the Social Security Act, privileged data and information, PSRO sanction reports and PSRO deliberations shall not be subject to subpeona or discovery proceedings in any civil action; nor shall any PSRO member, employee or consultant be subject to subpeona or discovery proceedings for the purpose of obtaining information relating to the above.

18. Disclosure: Claims Appeals

In claims appeals disclosure of privileged data or information to other than the claimant or his representative must be limited to those parties involved in the appeals process.

19. Disclosure: PSRO Deliberations

PSRO deliberations concerning patients, practitioners and facilities which serve as a basis of PSRO decisions shall not be disclosed outside the PSRO.

20. Disclosure: Sanction Proceedings

Subject to regulations governing administrative hearings under section 205(b) of the Social Security Act, and provisions for judicial review, privileged data and information and sanction reports may be disclosed for purposes of sanction proceedings, but disclosure is limited to physicians or facilities subject to sanction or their representatives, the appropriate Statewide Council for purposes of review and comment, and the Secretary or his authorized representatives for purposes of sanction determinations.

21. Disclosure: Results of Sanction Proceedings

If sanctions are levied on health care practitioners or health care providers by the Secretary pursuant to Section 1160 (b)(2), the name of the sanctioned party, the action taken and the nature of the sanction must be made a matter of public record by both the Secretary and the PSRO.

22. Disclosure: Monitoring, Review and Evaluation

For purposes of Federal and State program monitoring, review, and evaluation, privileged data and information may only be accessed by on-site visits to the PSRO or the other components of the PSRO review system in which the privileged data and/or information is stored. Privileged information or data may not be physically removed and/or transmitted outside of the PSRO review system except for the purpose of appeals or sanctions. Pursuant to paragraph #8 all privileged information and data needed for monitoring and program review purposes must contain all personal identification in a coded form.

23. Disclosure: Health Care Facility Information

Non-privileged data and information acquired and/or generated by any PSRO, its agents or ancillary components supporting PSRO review which is uniquely identifiable to a given health care facility may be disclosed upon request and payment of a fee to cover the expense of copying the requested information. However, the health care facility must be notified in writing 30 days prior to disclosure to permit the facility to review the information for accuracy and to provide comments to accompany the disclosed information.

24. Disclosure: Non-Privileged Information

Non-privileged information and reports generated within the PSRO may be disclosed to individuals, organizations and institutions upon request and payment of a fee to cover the expense of copying the requested information.

The following statement was adopted by an overwhelming majority of the Board:

A."Medical records, for these purposes, are any materials relating to a person's physical or mental health prepared for retention in permanent form in the possession of any custodian of medical records.

B. "Any person may, on request, have access to and the right to have copies of his/her own medical records in the possession of his/her doctor, a hospital or any other custodian of medical records.

C. "Persons other than the patient may have access to the patient's medical records only: (1) if the patient has given voluntary and informed consent in writing to the person seeking access or the release of records for a specific use, provided that the record will not be used for any other use; or(2) if the person claims access by virtue of a subpoena, of which the patient has been given notice and the usual opportunity to contest it prior to it's execution; or (3) if the records relate to a communicable disease that a health department or other government agency is required by law to identify and control, where the law forbids disclosure of this information for any other purpose and the patient, when possible, is given notice of the legal requirements; or (4) if material from the records is to be used in connection with medical or scholarly research, or publication of a case history, or any other related writing, in which event the identity of the patient must be disguised in accordance with appropriate professional standards, and subject to professional disciplinary review."

7. SUMMARY OF ETHICAL HEALTH DATA CENTERS CONCEPT

Brief Summary of the
Joint Task Group on Ethical Health Data Centers

The Joint Task Group was appointed in 1973, by the President of the Medical Society of the County of Erie, and by the Chairman of the Committee on Data Processing, Medical Society of the State of New York. The purpose was to form a multidisciplinary team to explore the potential utility of electronic data processing and related scientific disciplines, to examine the potential risks attached to computerization of sensitive clinical information.

The initial Joint Task Group included physicians, representatives of the regional nursing association and medical record association. Soon after the first meeting, the Health Sciences Faculty of the State University of New York at Buffalo offered support, and subsequently, other faculty members of the University joined the Task Group, providing their special expertise. The Task Group met regularly, every week. The various members had special background in ethics, broad competence in philosophy, law and jurisprudence, computer sciences, information retrieval, sociology, health care planning, and various areas related to health care. The Joint Task Group also invited experts from operating data systems with extensive data security measures.

The Joint Task Group's deliberations were summarized in their minutes, a 100 page document available to those interested in the problem of medical confidentiality. The Joint Task Group developed the following concepts and recommendations:

(1) information processing technology, when fully developed, will assist clinical medicine in decision making, it will close the gap between existing knowledge and bedside medicine, and it will assist the patient by maintaining a condensed, timely, pertinent medical history, genetic and social history;

(2) computer-based primary medical data must be effectively protected in order to maximize the benefits and to minimize the risks;

(3) for adequate protection of primary medical and related information ethical health data centers should be created, with a formal code of professional conduct, with explicit and appropriate operational standards, with clearly defined data access policies, and with adequate data security measures to provide medical confidentiality;

(4) such ethical health data centers should be the only acceptable way for handling confidential and potentially sensitive primary clinical data;

(5) the professional staff operating an ethical health data center shall have proven competence in information processing sciences and technology, integrity and moral obligation to provide medical privacy to those patients who have agreed to have their health-related data stored and processed;

(6) computer-based data handling operations which currently process potentially sensitive clinical information should be regulated as to data collection, access and information release, so as to conform with the ethical standards of practice of medicine;

(7) the Medical Society of the State of New York, in cooperation with other appropriate organizations, shall create an agency to inspect, accredit and regularly visit ethical health data centers located in New York State. The American Medical Association should make all the above a national policy;

(8) educational programs shall be created, without delay, for those physicians, nurses, medical record administrators, other health related professionals and information scientists who intend to staff ethical health data centers;

(9) effective public education shall be initiated to explain the value of confidentiality of medical records, to make the public aware of the emerging threats to medical privacy, and to inform the public what options are available for conserving the confidentiality of primary medical information;

(10) a legal framework shall be developed to protect the autonomy of ethical health data centers, and to impose punitive measures on violation of confidential, privileged medical information.

8.

GUIDELINES ON PRESERVING CONFIDENTIALITY OF MEDICAL RECORDS

National Association of Blue Shield Plans

Approved: September 3, 1975

The issue of confidentiality of medical records has become a major concern particularly with the passage of the Professional Standards Review Organization law and impending legislation for National Health Insurance. Physicians, health insurance carriers, government officials and others are concerned about the potential threat of indiscriminate access to, and releasing of, sensitive patient data.

From its inception, Blue Shield has functioned as a responsible third party in assuring the confidentiality of the physician-patient relationship. Its use of medical data has been for two essential purposes: assuring the patient's right to proper payment of medical care and the review of the appropriateness and necessity of care rendered by physicians and other health care providers.

By virtue of this inclusion into the relationship, Blue Shield believes it should state publicly its policy and outline its current procedures for maintaining the confidentiality of medical data.

BLUE SHIELD POSITION

It is Blue Shield's position that the confidentiality of medical information it accumulates as a medical prepayment organization must be assured. The consequence of improper disclosure of medical data entrusted to a Plan can be detrimental to the patient, the physician and the particular Blue Shield Plan.

Each Blue Shield Plan, therefore, has a legal and ethical responsibility to administer effective safeguards. The aim of these safeguards is to permit authorized access to the information while maintaining the integrity of the confidential relationship between patient, physician and Blue Shield.

GUIDELINES OF CONFIDENTIALITY

Blue Shield Plans have always administered procedures to safeguard medical information. The intent of the following guidelines is to suggest a review of those procedures already in existence or to implement programs which may be necessary to achieve the objective of assuring the confidentiality of medical information.

PUBLIC ACCESS AND RELEASE OF DATA

It should be recognized that a Blue Shield Plan is a third party to the patient-physician relationship. Since Blue Shield's file is a secondary or duplicate copy of the physician's primary record, there should be no need to inquire into Blue Shield's file. Patient inquiries, therefore, regarding medical data should be referred to the physician. However, Blue Shield may nonetheless become involved in a formal request. Therefore, the following guidelines should be applied:

1. In general, medical information should not be released without a court order. When under a court order to release certain medical information, the Blue Shield Plan should release only the specific information requested. Release of data beyond that which is requested is a violation of the confidentiality of the data.

2. Medical information should never be released over the telephone.

Although the Plan may be authorized to release information, it must not do so by telephone. The Plan has no proof that the person receiving the data is, in fact, the individual authorized to receive it.

3. Medical information may be released in the aggregate form, however, requests for such data should be in writing and should include the purpose for which the data will be used.

It is frequently necessary to release medical data for purposes of research for the study of utilization trends. The data must not, however, identify patient, subscriber or physician.

Additionally, the Plan must know who is requesting the information, and to the best of its ability, assure that the data will be utilized in a proper manner. No valid determination to permit or refuse release can be made without this data.

4. Medical information may also be released to the extent necessary for appropriate peer review bodies to assist in claims determination relative to costs and quality of care.

In these situations, patient identification should be deleted. In addition, physician identification should also be deleted unless a peer review organization deems it essential to the review. When the identity of the physician is essential, the physician should be notified.

ADMINISTRATIVE RESPONSIBILITY

1. The Chief Executive Officer should appoint specific officers or administrative employees who have the responsibility of authorizing release of medical information.

This assists the Plan in making certain that release of information has been properly authorized and reduces confusion over the requirements that must be met.

2. When in doubt, the Plan should rely upon its legal counsel to determine the appropriateness of a request for information and the extent of any release of medical data.

This assures the Plan that questionable requests receive the necessary legal considerations and that any release of information has met the proper legal requirements.

INTERNAL ACCESS AND HANDLING OF MEDICAL INFORMATION

1. Access to medical information should be limited to a "need to know" basis.

Confidential information implies restriction to the least number of people necessary. Indiscriminate access merely compromises those procedures intended to safeguard the data.

2. Adequate orientation and training programs should be developed and maintained which emphasize the sensitivity of medical records and the need to maintain their integrity.

The orientation and training program on the need to preserve confidentiality should be given high priority and consist of both oral and written presentations. In addition, periodic re-orientations on confidentiality of medical data should be conducted. If safeguards are not adequately met, an invasion of privacy may occur involving both the employee and the Plan.

3. Plan employees should seek only those data necessary to adjudicate a claim, case or utilization patterns and profiles.

   For example, if the Plan needs only a discharge summary or consultation report, it should not ask the hospital or physician for the entire record. To do so, not only creates storage problems, but also places unnecessary burdens on those mechanisms which are meant to insure confidentiality.

4. Adequate security precautions should be implemented to limit access to computers and data banks to those operating the systems.

   The massive amount of information collected by a Plan requires the use of automated data systems to perform its functions in an efficient and timely manner. This consolidation of data in computer storage banks or magnetic tapes facilitates easy access to, and retrieval of, information by anyone capable of operating the systems or copying tapes.

5. Employees should be encouraged to handle confidential data in a professional manner.

   Confidential information should not be discussed except for the purpose of adjudicating a claim.

In addition to a review of existing safeguard procedures, Plans are encouraged to communicate their activities to their subscribers and physicians. It is essential that their understanding and cooperation be gained in order that any procedures implemented by the Plan may be effecctively administered.

9. Policies and Recommendations for Policies, American Society of Internal Medicine

A. Statement on Confidentiality of Medical Records, Approved November, 1973

Background

Concerns relating to the confidentiality of medical records are increasing as the involvement of third parties in health care delivery is expanded. These concerns are heightened by poorly defined authorizations for release of information and by the increasing capability of machines for communicating interrelated identifiable patient information without the patient's knowledge and approval.

Evaluation

The right of the patient to confidentiality of his medical records is irrevocable. Third parties seeking any exception should be charged with the responsibility of fully informing patients of the possible consequences of such exceptions, and use by third parties of any privileged information must be limited to the purpose for which it was solicited.

Current laws do not adequately protect a patient's rights. The American Society of Internal Medicine believes that there is an immediate need for legislation which protects personal data on individual citizens and groups of citizens. We believe that there is a potential for personal injury or abuse by "authorized users."

Policy Statement

The American Society of Internal Medicine will work through the appropriate legislative channels and appropriate professional organizations for a law which will provide due process guarantees. These guarantees of confidentiality are to include security, accuracy, provision for change, knowledge of purpose, and informed permission for use.

B. Data Control by Government Programs

Background

There is a history of physician difficulty in obtaining data aggregated by government programs.

Evaluation

The government is increasingly involved in information gathering and there seems to be a natural tendency by those who pay for data to exercise total ownership prohibiting reasonable and necessary access. We are concerned about access to information generated in the process of medical care. We believe that access to data from federal programs must be provided in order that the data itself may be subjected to scrutiny regarding necessity, appropriateness and quality.

Policy

The American Society of Internal Medicine believes that the right of access to data by a data subject, either an individual or an organization, is irrevocable.

C. Excerpt from Proposed Policy for ASIM Contained in Report on Confidentiality, Conference Committee C, from Board of Trustees, February, 1975.

Definitions

1. The primary or permanent record belongs to the physician and his patient. It is the permanent data base which meets peer requirements for sufficiency and its release should not occur except with dual consent and then only for the purpose of treatment or patient management. The single exception to this consent requirement is the instance of legal action in which case record usage requires due process guarantees. The Primary Record may not contain notes made and retained by the physician solely for his personal use.

2. The active (working) record is the property of a physician and is solely for his personal use in connection with the diagnosis or treatment of a patient and is privileged unless such privileges are used to affect the patient's rights, benefits or liabilities, in which case its use is subject to due process requirements. The active record may contain notes which the physician intended solely for his own use.

3. Secondary data should be released only in a minimum set of data elements which will fulfill a "demonstrated need," and then only with the authorization of the data subject(s).

4. Certain secondary records used in audit or peer review should be privileged and prohibited from being admitted in court proceedings.

Life Span

1. The life span of an adult's permanent record should be no less than five years from the data of last activity (data entry) unless surgery has been performed. In this instance, it should be kept for at least ten years unless the patient dies. The record should be maintained for a period of (at least) two years after death.

2. The minor's permanent record should be maintained for at least five years after reaching adulthood. If surgery has been performed on a minor, the record should be preserved for a minimum of ten years after the patient becomes an adult under state law.

3. Primary medical records for mentally incompetent persons should be maintained throughout the individual's lifetime without regard to activity since statutory limitation may never prohibit suit for alleged malpractice.

4. The life span of a secondary record with patient identity should correspond exactly to the period required to accomplish specific objectives for which it was obtained.

10. Members of the NBS/ACM Workshop on Privacy, February 8-9, 1973

Chairman: Alan F. Westin, Professor of Public Law and Government, Columbia University, New York City

Stanley J. Aronoff, State Senator, Ohio

Melvin F. Bockelman, Computer Systems Division, Kansas City, Missouri Police Department

Walter M. Carlson, Corporate Consultant on Marketing, IBM Corporation

Russell L. Fenwick, Vice President, Bank of America, San Francisco

John L. Gentile, Deputy Director, Illinois Department of Finance

Lance Hoffman, Professor of Electrical Engineering & Computer Science, University of California, Berkeley

Seymour Jeffrey, Institute for Computer Sciences and Technology, National Bureau of Standards

Michael Kepplinger, Office of Computer Information, National Bureau of Standards

Paul F. Krueger, Deputy Chief, Statistical Policy Division, U. S. Office of Management & Budget

Dr. Peter G. Lykos, Program Director, Special Research Resource, National Science Foundation

David B. H. Martin, Executive Director, Committee on Automated Personal Data Systems, Department of Health, Education and Welfare

Anthony G. Oettinger, Professor of Applied Mathematics, Harvard University

James E. Riley, Legal Counsel, UNIVAC, Blue Bell, Pennsylvania

Herbert Saxon, Manager, Public Safety & Civil Systems Department, System Development Corporation, Santa Monica, California

John H. F. Shattuck, American Civil Liberties Union, New York City

Rein Turn, Rand Corporation, Santa Monica, California

11. Persons Attending Draft Report Review Conference, September 16-17, 1975, Gaithersburg, Maryland

Chairman: Dr. Vernon Wilson, Vanderbilt University, Nashville, Tennessee

Robert R. Belair, Domestic Council Committee on the Right of Privacy

Colonel Rudolph G. Bickel, M.D., U. S. Air Force

Mary Converse, Bureau of Professional Services, American Hospital Association

Robert H. Courtney, Manager, Data Security and Privacy, IBM Corporation

Royal Crystal, Bureau of Quality Assurance, Department of Health, Education, and Welfare

Hope Eastman, Associate Director, Washington Office, American Civil Liberties Union

John P. Fanning, Special Assistant to the Director, Office of Policy Development & Planning, Office of the Assistant Secretary for Health

Maurice Grossman, M.D., Clinical Professor of Psychiatry, Stanford University

Daniel K. Harris, American Medical Association

Carnault Jackson, M.D., San Antonio, Texas

David B. H. Martin, Administrative Conference of the United States

Peter F. McCloskey, President, Computer and Business Equipment Manufacturers Association

Dr. Robert H. Mugge, National Health Center for Health Statistics Public Health Service, U. S. Department of Health, Education and Welfare

Carole Parsons, Executive Director, Privacy Protection Study Commission

Elaine O. Patrikas, Chair, Department of Health Records Administration, College of Allied Health Professions, Temple University

Elizabeth Price, Director, Professional Services, American Medical Records Association

Jack Richardson, IBM Corporation

Quincy Rodgers, Executive Director, Domestic Council Committee on the Right to Privacy

Walter Rubenstein, Social Security Administration

Vergil N. Slee, M.D., President, Commission on Professional and Hospital Activities

Joseph Terdiman, Kaiser Hospital, Oakland, California

Willis Ware, Rand Corporation, Santa Monica, California

Lawrence L. Weed, M.D., Director, PROMIS Laboratory, University of Vermont, Burlington, Vermont

From the Medical Records Project Staff:

Alan F. Westin
Michael A. Baker
Helene Toiv

From the National Bureau of Standards:

Ruth M. Davis
Seymour Jeffrey
Michael Kepplinger
John L. Berg

12. GENERAL ACKNOWLEDGMENTS

In addition to those persons already acknowledged in the Preface, and those noted in the references to the profiles, the following persons aided in our researches, helped review our drafts, or supplied us with valuable materials.

From IBM, Jack Richardson, Dr. John Duffy, Jerry G. Anderson, Bud Enright, Bob Kukla, Gail Agnew, Robert Hoynes, Kent Goode, and Robert Courtney; from Honeywell, Robert Henderson, E.P. DiCostanzo, Art Hill, Duane Sutfin, J. Turner, J. Mahoney, and E. Howell; and from Sperry Univac, Fred Anderson, R.B. Batman, James E. Riley, and R. Parratt (Sperry Univac International Executive Centre, Rome).

From the American Civil Liberties Union, Hope Eastman, John H.F. Shattuck, Trudy Haydn, Jeremiah Gutman, Anne Prichard, Lauren Selden, Florence Wills, Charles Marson, David Addlestone, John Roemer III, Kenneth P. Norwick, Jay Hartwell, Robert S. Howe, Frank Cochran, Dororthy D. Davidson, Roberta Marks, William H. Lynch, Gordon Beggs, Brent A. Barnhart, Ira Glasser, Barbara Bernstein, Diana H. Josephson, Stevie Remington, Philip Boxell, Lawrence Faulkner, Bruce Ennis, and Howard Simon.

And from various organizations and institutional affiliations, Dr. Adele Hoffman, Alan Sussman, Leonard H. Glantz, Robert Ellis Smith, Dr. Raymond E. Vath, Martin D. Capell, Frank A. Schneiger, John Vanderstar, Dr. Dan Klein, Marjorie Eltzroth, Anthony G. Oettinger, Launor F. Carter, Robert M. Veatch, Vergil N. Slee, Lance O. Hoxie, Dr. Simon Auster, Elaine O. Patrikas, Barbara Kaiser, Hannah A. Achtenberg, Barbara Puder, Dr. Daniel K. Harris, Dr. Maurice Grossman, Dr. Herbert Sacks, Ruby Okubo, Frederic G. Withington, Dr. Paul S. Entmacher, Howard H. Hiatt, Lawrence C. Morris, Jr., Dr. Leonti H. Thompson, Dr. Laurence Weed, John H. Noble, Jr., Verne R. Kelley, Hannah B. Weston, Catherine E. Rosen, William H. Calvin, John Fanning, Willis H. Ware, David B.H. Martin, Susan Bennett, Robert Belair, Quincy Rogers, Carole Parsons, Ronald Plesser, A. Lee Lester, Walter F. Bauer, Dr. Michael A. Jenkin, Gus Stuhldreher, Frank E. Heart, Alan Meisel, Nathan Stark, H.G. Pearce, Dr. Joseph F. Terdiman, Dr. Donald A. B. Lindberg, Lawrence White, John De Leo, Margaret Kilduff, Peter Bornstein, Jonathan Brant, Royal Crystal, Martin Berck, Ronald Sullivan, Cindy Fanto, Donna Gane, Charles C. Clarke, Howard Walderman, Lorraine Volz, Franklin Reeder, James H. Moore, Robert A. Driscoll, William Kingsley, Erica Grubb, Lottie Gottschalk, Len J. Tondl, William B. Swarts III, E. M. Steindler, Dr. Eli Sorkow, William B. Smith, Dr. Robert S. Long, J. J. Lavoie, Eugene Laska, Rheta Bank, John A. Kirchbaum, and Hans Gassmann.

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM. **BIBLIOGRAPHIC DATA SHEET**	1. PUBLICATION OR REPORT NO. NBS Monograph 157	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

Computers, Health Records
and Citizen Rights

5. Publication Date
December 1976

6. Performing Organization Code

7. AUTHOR(S)
Alan F. Westin

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

Department of Political Science
Columbia University
New York, New York 10027

10. Project/Task/Work Unit No.
640.1116

11. Contract/Grant No.
5-35886

12. Sponsoring Organization Name and Complete Address (Street, City, State, ZIP)

National Bureau of Standards
Department of Commerce
Washington, D.C. 20234

13. Type of Report & Period Covered
Final

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 76-608322

16. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

This report investigates the impact of computers on citizen rights in the health record-keeping area. Under Dr. Alan F. Westin's direction, from July of 1974 to April of 1976, a small interdisciplinary team did the following: (1) examined published literature from medicine and health, law, computing, and social science; (2) conducted interviews with major computer manufacturers, systems developers, health professionals and civil liberties, public interest, consumer, and minority-rights groups; (3) made on-site visits to six representative health-care organizations using computers to handle personal records; (4) corresponded with 70 organizations in the health field; and (5) subjected an initial draft report to review by a conference of experts in September 1975 and subsequently by about 50 outside reviewers. The findings of this investigation were then combined into this four-part report. Part One describes the world of medical data and citizen rights within the framework of three zones--primary health care (by health professionals), service payers and health care reviewers, and social uses of health data (such as in employment, life insurance, and welfare); Part Two treats patterns of computerization in health care in each of the above zones; Part Three contains the profiles of the six health-care organizations that were studied in depth; and Part Four analyzes the impact of computerization on personal health records, presents comparisons with six other democratic nations, and states 12 recommended management principles for health care data systems. The report also contains a 28 page bibliography and twelve appendices with support documents and information.

17. KEY WORDS *(six to twelve entries; alphabetical order; capitalize only the first letter of the first key word unless a proper name; separated by semicolons)* Citizen rights; computers; confidentiality; data systems; health records; information policy; management principles; medical records; privacy; record-keeping practices; security.

18. AVAILABILITY ☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☒ Order From Sup. of Doc., U.S. Government Printing Office
Washington, D.C. 20402, SD Cat. No. C13.44:157

☐ Order From National Technical Information Service (NTIS)
Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT) UNCLASSIFIED	21. NO. OF PAGES 401
20. SECURITY CLASS (THIS PAGE) UNCLASSIFIED	22. Price $4.55

USCOMM-DC 29042-P74

U. S. GOVERNMENT PRINTING OFFICE : 1976 O - 225-346

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH reports National Bureau of Standards research and development in physics, mathematics, and chemistry. It is published in two sections, available separately:

- **Physics and Chemistry (Section A)**

Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

- **Mathematical Sciences (Section B)**

Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

DIMENSIONS/NBS (formerly Technical News Bulletin)—This monthly magazine is published to inform scientists, engineers, businessmen, industry, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on the work at NBS. The magazine highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, it reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing.

Annual subscription: Domestic, $9.45; Foreign, $11.85.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a world-wide program coordinated by NBS. Program under authority of National Standard Data Act (Public Law 90-396).

NOTE: At present the principal publication outlet for these data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St. N.W., Wash. D. C. 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The purpose of the standards is to establish nationally recognized requirements for products, and to provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order **above** *NBS publications from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.*

Order **following** *NBS publications—NBSIR's and FIPS from the National Technical Information Services, Springfield, Va. 22161.*

Federal Information Processing Standards Publications (FIPS PUBS)—Publications in this series collectively constitute the Federal Information Processing Standards Register. Register serves as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Services (Springfield, Va. 22161) in paper copy or microfiche form.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service. A literature survey issued biweekly. Annual subscription: Domestic, $20.00; Foreign, $25.00.

Liquified Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $20.00. Send subscription orders and remittances for the preceding bibliographic services to National Bureau of Standards, Cryogenic Data Center (275.02) Boulder, Colorado 80302.